JOSCM Journal of Optimization and Supply Chain Management
Print ISSN:3079-1022 Online ISSN:3079-1030

AI-Enabled Decision-Making and Governance Risk in Global Supply Chains: Frameworks for Accountability, Transparency, and Resilience

Valentina Ochuko Obukadata[1], Chukwudera Anunagba[2]✉, Shalom Alugwe[3], Serif Oyindamola Oyesiji[4], Kingsley Chinazaekpere Ndupu[5], Harouna Wendpanga Yann Christian Sankara[6], Toussida Fatah Tanguy Minoungou[6], Uchechukwu Nkechinyere Anene[7]

1. Pompea College of Business, University of New Haven, West Haven, Connecticut, USA. E-mail: vobuk1@unh.newhaven.edu
2. Corresponding author, Barclays, Whippany, New Jersey, USA. E-mail: chukwudera.anunagba1@barclays.com
3. Independent Researcher, USA. E-mail: shalomalugwe@gmail.com
4. Harrisburg University of Science and Technology, Harrisburg, Pennsylvania, USA. E-mail: oyesijiserif@gmail.com
5. Kennesaw State University, Kennesaw, Georgia, USA. E-mail: kingsleynd34@gmail.com
6. Independent Researcher, Dallas, Texas, USA. E-mail: christiansankara@gmail.com; tanguyminoungou@gmail.com
7. Kellstadt Graduate School of Business, DePaul University, Chicago, Illinois, USA. E-mail: uanene@depaul.edu

Article Info

Article type:
Review Article

Article history:
Received September 5, 2026
Received in revised form October 16, 2026
Accepted November 5, 2026
Available online November 13, 2026

***Keywords*:**
artificial intelligence governance
supply chain decision-making
algorithmic accountability
transparency
supply chain resilience

ABSTRACT

Objective: Artificial intelligence in global supply chains has moved from analytical aid to executing authority, selecting suppliers, rerouting freight, and screening counterparties with little human intervention. This review characterizes the resulting governance risk: the risk that an organization cannot explain, justify, contest, correct, or answer for a decision taken through its automated systems.

Methods: A structured narrative review with a disclosed protocol synthesized 119 sources, comprising 101 studies and instruments published between 2018 and 2026 and 18 earlier foundational works, identified through five databases, targeted regulatory retrieval, and snowballing. A governance framework was then developed by design synthesis.

Results: Accountability structures rarely track the actual locus of decision, and advisory systems with high acceptance rates function as delegated systems with advisory-grade protections. Seven mechanisms generate governance risk, notably epistemic opacity, accountability diffusion, algorithmic monoculture, and displaced coercion onto lower-tier suppliers. The proposed Governed Autonomy Framework has four layers (decision rights and authority tiering, evidentiary traceability, assurance and contestability, and resilience engineering), operationalized through a five-level maturity model, governance indicators, and a staged implementation path.

Conclusion: Governance risk is separable from model and operational risk and poorly addressed by prevailing compliance architectures. Supplier contestability is the most valuable and most neglected control, justified epistemically rather than ethically. Current regulatory deferrals do not justify delaying the evidentiary work that later compliance will require.

Cite this article: Obukadata, V. O., Anunagba, C., Alugwe, S., Oyesiji, S. O., Ndupu, K. C., Sankara, H. W. Y. C., Minoungou, T. F. T., & Anene, U. N. (2026). AI-Enabled Decision-Making and Governance Risk in Global Supply Chains: Frameworks for Accountability, Transparency, and Resilience. *Journal of Optimization and Supply Chain Management*, *XX*(X), pages. https://doi.org/10.22034/ISS.2026.11473.1101

© Author(s) retain the copyright.
Publisher: International Scientific Services (ISS)
DOI: https://doi.org/10.22034/ISS.2026.11473.1101

1. Introduction

For most of the past two decades, artificial intelligence in supply chain management was a discussion about forecasting. Better demand signals, better lead-time estimation, better anomaly detection in quality data. The governance question raised by such systems was narrow: how accurate is the model, and how far should the planner trust it? Responsibility remained unambiguously human, because a human sat between the model output and the consequence (Baryannis et al., 2019; Choi et al., 2018).

That intermediate position is being removed. Deployments now involve goal-directed systems that monitor operational data continuously, reason across workflows, and execute within a defined authority envelope without seeking approval at each step. Procurement systems issue requests for quotation, evaluate bids, and update systems of record (Ahiaeke Patrick et al., 2021; Akinleye & Adeyoyin, 2021). Planning systems sense demand and reposition inventory (Aifuwa et al., 2020; Akin-Oluyomi, Atima, Akinleye, & Okoruwa, 2023). Risk systems scan supplier financial signals, geopolitical events, certification status, and news sentiment, then recommend or initiate sourcing changes (Filani et al., 2022; Nnabueze et al., 2021). Warehouse fleets coordinate through multi-agent controllers with no operator in the execution path (Akanbi et al., 2025; Akanbi & Sunday, 2024, 2025; Huertos et al., 2026; Kumar et al., 2026), and orchestration architectures now extend agentic execution across enterprise boundaries (Ogundairo, 2025).

The operational case is well evidenced in mainstream, database-indexed reviews. Systematic reviews of AI adoption across supply chain functions report consistent gains in resilience, cost control, and continuity (Shahzadi et al., 2024; Zamani et al., 2023). A cluster of applied, practitioner-oriented studies reports comparable gains at finer operational grain: digital supply chain governance models in cost control and cycle time (Okonkwo et al., 2024a, 2024b, 2024e), predictive procurement planning sustaining operational uptime (Okonkwo et al., 2024c), automation and digital twins reducing procurement errors and turnaround (Akinlade et al., 2024; Akinleye & Adeyoyin, 2021), integrated digital platforms improving transparency across procurement networks (Okoruwa et al., 2024, 2025), and procurement strategy and enterprise resource planning adoption at national scale (Okonkwo et al., 2024d, 2025). This second cluster is treated throughout this paper as illustrative deployment texture rather than as independent corroboration, for the reasons made explicit in Section 2.3. The difficulty is that the control architecture surrounding these systems, however evidenced, has not kept pace with the authority delegated to them. Organizations have installed machine agency inside governance structures designed for human agency, and the mismatch is where exposure accumulates.

This paper defines governance risk as the risk that an organization cannot explain, justify, contest, correct, or answer for a consequential decision taken through or by its automated systems. The definition draws on the structural account of accountability as a relationship in which an actor is obliged to explain conduct to a forum that can question, judge, and impose consequences (Bovens, 2007), and it is institutional rather than technical. A perfectly accurate model can still generate severe governance risk. This happens if no one can reconstruct why it acted, if no affected party can challenge the outcome, if responsibility is contested between the deploying business unit, the internal data team, and an external vendor, or if the decision cannot be reversed within the time the harm takes to materialize. Conversely, a mediocre model inside a strong accountability architecture may present modest governance risk, because errors surface, ownership is clear, and remedies exist. Governance risk is therefore a property of the sociotechnical assembly rather than of the model artefact, which implies that improvements in model performance are not substitutes for improvements in institutional structure.

Three features make supply chains a harder governance environment than the settings in which algorithmic accountability has mostly been studied. Decisions extend across organizational boundaries and land on legally independent enterprises that did not consent to the model and cannot inspect it. Algorithmic accountability scholarship developed largely around decisions made by an institution about individuals within its own jurisdiction (Diakopoulos, 2016; Mittelstadt et al., 2016; Pasquale, 2015), whereas supply chain decisions concern independent firms, many of them small and several contractual removes from the decision-maker (Tachizawa & Wong, 2014; Villena & Gioia, 2018). Multi-tier networks are informationally dark below the first tier, so models are most confident where visibility

is best and least reliable where risk concentrates (Akin-Oluyomi et al., 2023b; Nnabueze et al., 2021). And supply networks are tightly coupled in the sense developed for high-risk technologies, so that buffers are thin by design and local adjustments propagate (Kim et al., 2015; Perrow, 1984). When many firms deploy similar models on overlapping data the network acquires a shared reflex with no analogue in a population of independently deliberating planners (Agbabiaka et al., 2019; Ogunwole et al., 2021).

The paper addresses four questions. Which configurations of AI decision authority are being deployed, and where does accountability actually sit? Through what mechanisms does AI-enabled decision-making generate governance risk in multi-tier networks? What structural features must an accountability framework possess when decision authority is delegated across organizational boundaries? And how can such a framework be operationalized while regulatory obligations expand and enforcement deadlines move?

Section 2 sets out the review protocol and the framework development method. Section 3 presents the taxonomy, the mechanisms, the regulatory position, the proposed framework, and its operationalization. Section 4 discusses cross-cutting findings, implications, and limitations. Section 5 concludes.

2. Materials and Methods

2.1 Design

The study combines a structured literature review with conceptual framework development. The review draws on the reporting principles of PRISMA 2020 for eligibility criteria, transparency of source classification, and disclosure of search construction (Table 1), but it is reported as a structured narrative review with a disclosed protocol rather than as a formal PRISMA systematic review, for reasons stated here rather than left implicit. Three features of the evidence base make a single linear PRISMA flow diagram unsuitable. The corpus spans three evidence classes identified through different routes: database search, targeted retrieval of standards and regulatory instruments, and backward and forward snowballing from included studies (Section 2.2). The applied and practitioner literature entered predominantly through snowballing and citation-network inspection rather than through the five named databases directly, so a single count of records identified per database would misstate its actual provenance. And snowballing continued iteratively as the framework in Section 3.4 was developed, rather than terminating in a single discrete screening pass before synthesis began. Section 2.2 reports the search constructs and the screening process used, Section 2.3 states how the resulting three evidence classes are composed and weighted, and Section 2.4 discloses the limits this reporting choice places on reproducibility. The framework itself is developed by design synthesis: each mechanism identified in the review generates a control requirement, and the requirements are grouped into layers ordered by dependency. This is a theory-building rather than a theory-testing design, and Section 4.6 states the resulting limitations. Where controls are proposed they are aligned to established risk and assurance instruments so that adoption can proceed within existing management systems (International Organization for Standardization [ISO], 2018; International Organization for Standardization & International Electrotechnical Commission [ISO/IEC], 2023; National Institute of Standards and Technology [NIST], 2023).

2.2 Search strategy and eligibility

Searches were executed across Scopus, Web of Science, IEEE Xplore, the ACM Digital Library, and ScienceDirect, supplemented by targeted retrieval of standards and regulatory instruments and by backward and forward snowballing from included studies. Table 1 records the construction. The window opens in January 2018 and closes in July 2026.

Table 1. Search strategy across evidence sources

Source	Coverage	Primary query construct
Scopus; Web of Science	Operations, information systems, and management venues	("supply chain" OR procurement OR logistics) AND ("artificial intelligence" OR "automated decision" OR algorithmic) AND (governance OR accountability OR risk)
IEEE Xplore; ACM Digital Library	Computing, accountability, and human-factors venues	("algorithmic accountability" OR "automated decision-making" OR "human-in-the-loop" OR "agentic") AND (transparency OR audit OR oversight)
ScienceDirect	Resilience, due diligence, and multi-tier governance	("supply chain resilience" OR "multi-tier" OR "due diligence") AND (disruption OR visibility OR supplier)
Standards and regulatory portals	Binding and normative instruments	Named-instrument retrieval: EU AI Act, CSDDD, ISO 31000, ISO/IEC 42001, NIST AI RMF, UNGP, OECD guidance
Applied and practitioner literature	Deployment evidence in procurement and logistics	(procurement OR "digital supply chain" OR "supplier risk") AND (automation OR analytics OR "digital twin" OR platform)
Snowballing	Backward and forward	Reference lists and citing works of all included studies

Records were included where they addressed automated or algorithmic decision-making in supply chain, procurement, or logistics settings; accountability, transparency, or resilience of automated systems; or governance and regulatory instruments bearing on either. Records were excluded where they addressed model performance with no governance dimension, or where full text was unavailable.

Title and abstract screening, and eligibility coding of retrieved full texts, was conducted independently by two co-authors, Chukwudera Anunagba and Serif Oyindamola Oyesiji, against these criteria; disagreements were resolved by discussion, with a third co-author, Kingsley Chinazaekpere Ndupu, adjudicating where discussion did not converge. Snowballing substantially supplemented the five named databases: a majority of the applied and practitioner-tier sources entered the corpus through citation-network inspection of included studies and of a small number of research groups publishing recurrently on operational AI deployment in procurement and logistics, rather than through direct retrieval from Scopus, Web of Science, IEEE Xplore, the ACM Digital Library, or ScienceDirect. Where a retrieved source's journal could not be confirmed as indexed in one of the five named databases, it was coded as applied or practitioner-tier evidence (Section 2.3) rather than as an indexed peer-reviewed source, irrespective of that journal's own claim to operate peer review.

2.3 Corpus and synthesis

The final corpus comprises 119 sources. Sources were assigned to an evidence class by an explicit, applied rule rather than by a scored quality-appraisal instrument: a source was classed as an indexed peer-reviewed study only where its journal could be confirmed as covered by Scopus, Web of Science, IEEE Xplore, the ACM Digital Library, or ScienceDirect at the time of coding; a source was classed as a standard, regulatory, or intergovernmental instrument where it was issued by a standards body, regulator, or intergovernmental organization; a source was classed as a scholarly monograph where it was a book from an academic or university press; and every remaining source, including journals that describe themselves as peer-reviewed but could not be confirmed as indexed, was classed as applied or practitioner-tier evidence. On this rule the corpus comprises 37 indexed peer-reviewed journal articles, 4 scholarly monographs, 8 standards or regulatory instruments, and 70 applied or practitioner-tier journal articles (59% of the corpus), the last concentrated in a recurring set of operations- and compliance-focused journals and a recurring set of co-authoring research groups; Section 2.4 states the resulting limitation explicitly. Indexed peer-reviewed studies carry the greatest weight in claims about mechanism and are used, wherever available, as the anchor citation for a claim. Standards and regulatory instruments are treated as authoritative for normative content and non-authoritative for effectiveness. Applied and practitioner-tier studies are used for illustrative deployment texture and for the operational feasibility of controls, and are not treated as independent corroboration of a claim that also requires an indexed source.

Synthesis was narrative and thematic rather than meta-analytic, because outcome measures across the corpus are too heterogeneous to pool.

2.4 Threats to validity

Five limitations qualify the findings. Publication bias is material, since failed deployments and suppressed disputes are largely absent from the record. Sector bias is present, because the applied evidence concentrates in energy, infrastructure, pharmaceutical, and retail supply chains, and conclusions may not transfer to sectors with different contracting norms. Recency bias affects the agentic and multi-agent literature, where deployment is running ahead of evaluation. Citation-base composition is a further limitation. Of the 119 sources, 37 are journal articles in venues confirmed as indexed in one of the five named databases, 4 are scholarly monographs from established academic presses, 8 are standards, regulatory, or intergovernmental instruments, and 70 (59%) are applied or practitioner-tier journal articles whose indexing in the five named databases could not be confirmed, with a recurring set of co-authoring research groups accounting for a large share of this last category. These sources are treated throughout as illustrative deployment texture rather than as independent corroboration (Section 2.3), but the paper's account of the scale and maturity of operational AI deployment in supply chains would rest on a narrower evidentiary base if this category were removed, and readers should weigh the applied evidence accordingly. Reproducibility is correspondingly limited. Because identification combined database search with extensive iterative snowballing across heterogeneous evidence classes (Section 2.1), stage-by-stage screening counts were not tracked in a form that supports a single PRISMA flow diagram; the eligibility criteria, screening process, and evidence-class composition reported in Sections 2.2 and 2.3 are offered in place of that diagram. Finally, the regulatory account in Section 3.3 reflects instrument texts and amendments as verified against official sources up to the July 2026 search cut-off stated in Section 2.2. This area is under active amendment, and readers relying on this account for compliance purposes should verify current requirements against the primary regulatory texts rather than against this account.

3. Results

3.1 A taxonomy of AI decision authority

Governance requirements depend less on model architecture than on where the decision actually resides. Table 2 distinguishes four configurations.

Table 2. Configurations of AI decision authority in supply chains

Configuration	Machine function	Human function	Locus of decision	Illustrative use
A. Descriptive	Aggregates and reports	Interprets and decides	Human	Spend dashboards; tier-one visibility maps
B. Advisory	Predicts and recommends	Evaluates and decides	Human, but anchored by the recommendation	Demand forecasting; supplier scorecards
C. Delegated	Decides and executes within bounds	Sets bounds; reviews exceptions; audits after the fact	Machine, within a human-set envelope	Automated replenishment; freight rebooking; spot buying
D. Autonomous	Sets sub-goals; coordinates with other agents; executes	Sets objectives; monitors aggregate outcomes	Machine, distributed across agents	End-to-end orchestration across procurement, logistics, and finance

The literature has concentrated on the advisory configuration, where explanation supports a human judgement. Deployment has moved to delegated execution and is entering autonomous orchestration (Akanbi et al., 2025; Ogundairo, 2025), where explanation must instead support reconstruction of a decision already taken and executed.

The advisory configuration is less protective than it appears. Advisory systems produce a default, and defaults are sticky. When a recommendation arrives with a confidence score and an accept control, the marginal cost of acceptance approaches zero while rejection costs analysis time and personal exposure if the override proves wrong. Under production conditions an advisory system with a high acceptance rate is functionally a delegated system carrying

advisory-grade protections, which is the least defensible combination available: real machine authority with nominal human accountability. Organizations should therefore classify systems by observed override rate rather than by design intent. This is the configuration in which the human operator absorbs blame for failures they had no realistic capacity to prevent (Elish, 2019; Wagner, 2019). Human oversight requirements fail in practice for the same reason, namely that the reviewer lacks the time, information, incentive, or authority to override (Green, 2022; Green & Chen, 2019; Ladapo et al., 2022, 2024).

Authority also migrates without deliberate decision. A model is deployed as advisory; performance is good and trust accrues; a threshold is introduced so that low-value or high-confidence cases pass without review, justified as efficiency rather than as a transfer of authority; the threshold is raised; scope extends to adjacent categories; and integration with the enterprise resource planning system allows the model to write rather than only read, at which point recommendation becomes execution (Okonkwo et al., 2024f, 2023). Figure 1 shows the sequence. At no point does a governance body approve a delegation, because no single step appears to constitute one. Governance risk accumulates in the gaps between increments, which is why Layer 1 of the framework makes authority allocation an explicit and periodically reauthorized act.

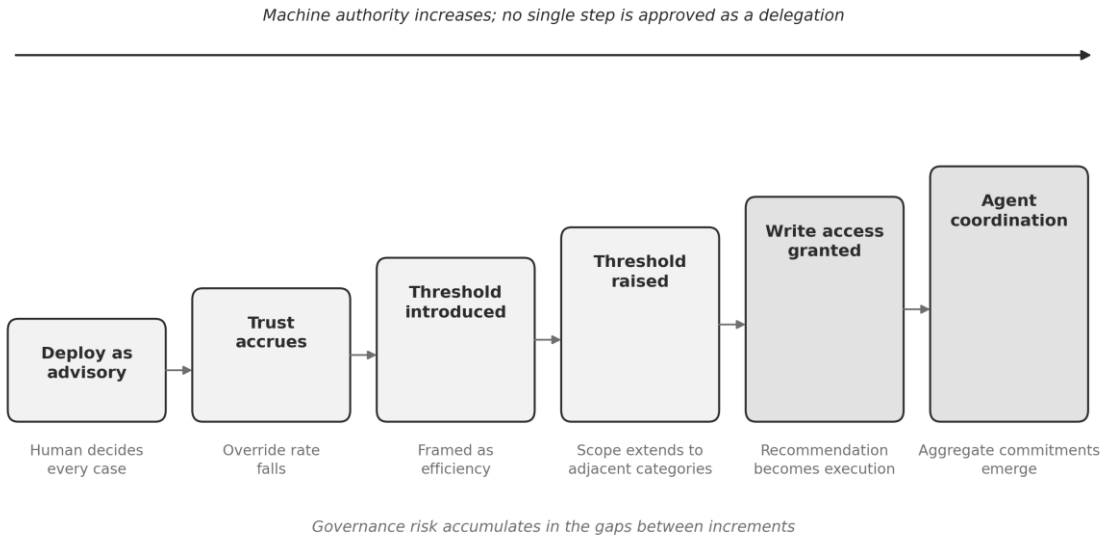


Figure 1. Drift of decision authority from advisory recommendation to autonomous execution.

3.2 Mechanisms of governance risk

Table 3 summarizes seven mechanisms. They are analytically distinct and require different controls, but in deployed systems they compound.

Table 3. Mechanisms of governance risk

Code	Mechanism	Generating condition	Primary consequence
M1	Epistemic opacity	Inputs systematically weakest where risk concentrates; confidence diverges from validity	Unjustified precision; low scores in unobserved network regions
M2	Accountability diffusion	Responsibility fragments across vendor, function, jurisdiction, and counterparty seams	Elastic accountability; no forum can compel a complete account
M3	Inherited data liability	Provenance of training and operating data not controlled by the deployer	Legal, evidential, and contaminative exposure

Code	Mechanism	Generating condition	Primary consequence
M4	Algorithmic monoculture	Common vendors, models, and signal providers across competing firms	Synchronised exit; convergent sourcing; reflexive amplification
M5	Displaced coercion	Optimisation pressure transmitted to suppliers with limited absorptive capacity	Adverse human rights impact invisible to the deploying system
M6	Jurisdictional fragmentation	Divergent definitions, obligations, and timetables across regimes	Segmented deployment; arbitrage; deferral
M7	Model supply chain concentration	Few providers of models, platforms, and commercial risk data	Unnotified behavior change; irreproducible decisions; sectoral correlation

Epistemic opacity. Even a fully interpretable model produces unjustified confidence when its inputs are structurally unrepresentative of the phenomenon assessed. A supplier risk score drawn from audit records, self-declarations, certification databases, trade data, and media monitoring learns to predict detected and documented risk, and will assign low scores to opaque regions of the network because opacity resembles absence in the training data. The output carries an implied precision the evidence cannot bear, and once it enters a workflow it acquires an authority the qualitative judgement it replaced never had, because it arrives without a visible author. Opacity of this kind is intrinsic to the scale and character of machine learning rather than a product of concealment (Burrell, 2016), and it is compounded because private audit documentation is itself an unreliable signal of conditions on the ground (LeBaron & Lister, 2015; Locke, 2013). Visibility research reaches the compatible conclusion that disclosure frameworks deliver value only where the underlying data actually reach the tiers that matter (Abioye et al., 2023; Akin-Oluyomi et al., 2023b; Nnabueze et al., 2021).

Accountability diffusion. Responsibility fragments along at least five seams: between vendor and deployer, between model provider and application vendor, between business and technical functions, between buyer and supplier, and across legal entities and jurisdictions. This is the problem of many hands, in which computerized systems distribute causal contribution so widely that no single party can be held responsible (Nissenbaum, 1996). The consequence is not the absence of accountability but its elasticity, since every party can construct a defensible account in which the decisive contribution lay elsewhere. Work on algorithmic accountability and model risk management in regulated industries identifies the same fragmentation and proposes assignment in advance rather than attribution after the event (Ominyi & Anichukwueze, 2023, 2024; Ominyi et al., 2026b).

Inherited data liability. Systems are trained and operated on data whose provenance the deploying firm did not control. Supplier-submitted documentation, third-party risk databases, purchased datasets, and scraped content each carry potential defects in licensing, legal basis, and accuracy. Three exposures follow: legal, where personal data of supplier personnel crosses jurisdictions with divergent transfer rules (Annan, 2022; Ominyi & Anichukwueze, 2022a); evidential, where undocumented provenance cannot demonstrate that diligence was adequate (Aneke et al., 2023); and contaminative, where erroneous data propagate into decisions that cannot be traced back to the originating record. Dataset documentation practice exists precisely to make these properties inspectable before deployment (Gebru et al., 2021).

Algorithmic monoculture and correlated failure. Competing firms procure comparable systems from a small number of vendors, built on fewer foundation models, fed by common signal providers. Three effects follow. Synchronized exit occurs when a supplier flagged by one buyer is flagged by all, near simultaneously, possibly on an error no single buyer has an incentive to investigate. Convergent sourcing means diversification measured at firm level coexists with concentration at sector level, since optimizers pointed at similar objectives on similar data recommend similar alternatives. Reflexive amplification occurs when many autonomous systems detect the same disruption signal and respond within minutes, so that the aggregate response exceeds the initiating shock. Human procurement organizations respond over days with heterogeneous judgement, which damps propagation; machine response is fast and homogeneous, which amplifies it. Formal analysis shows that algorithmic monoculture can reduce aggregate outcome quality even where each individual algorithm outperforms the human judgement it replaces, because correlated selection destroys the diversifying benefit of independent error (Kleinberg & Raghavan, 2021), and the

financial sector has already encountered the systemic form of this dynamic (Danielsson et al., 2022). This exposure is generated by the correlation structure of the sector rather than by any firm's own configuration, which is why it cannot be managed at firm level alone.

Displaced coercion. Optimization exerts pressure that terminates in workplaces the deploying firm cannot see. Dynamic lead-time compression, algorithmically determined order variability, and automated penalty enforcement transmit demands to suppliers whose capacity to absorb them is limited; the supplier meets them through overtime, subcontracting, or informal labour; the buyer's system records on-time delivery and improves the supplier's score. Two features make this worse under automation than under human purchasing. Optimization operates continuously and at the boundary of feasibility, removing slack that human buyers left in place through inattention or relationship management (Ike et al., 2021, 2022). And the causal chain from objective function to labor practice is long enough that no individual decision appears to be a decision about working conditions at all. A purchasing algorithm that systematically contributes to excessive working hours is a contribution to adverse impact within the meaning of established due diligence standards, regardless of intent (Organization for Economic Co-operation and Development [OECD], 2018, 2023; United Nations, 2011), yet few firms assess their own purchasing algorithms as a due diligence subject. Automated systems producing differential outcomes for identifiable groups also attract direct compliance exposure (Annan, 2025a; Ominyi & Anichukwueze, 2024).

Jurisdictional fragmentation. A single system may be subject to European AI regulation, sectoral rules, export controls, data protection law in several jurisdictions, and national due diligence statutes, which define regulated activity differently and apply on incompatible timetables (Annan, 2022; Ominyi & Anichukwueze, 2022a; Ominyi et al., 2024b). Fragmentation drives geographic segmentation of deployment, which defeats the network-level visibility that motivated the system, and invites deferral, which is itself a governance failure while the underlying activity continues. Sector-specific disclosure regimes add a further layer where environmental and social reporting obligations intersect with automated data collection (Ominyi & Anichukwueze, 2022b), and confidentiality constraints on enterprise language model deployment restrict what may lawfully be recorded in a decision log (Ominyi et al., 2025c).

Concentration in the model supply chain. Firms conduct extensive diligence on suppliers of physical components and comparatively little on suppliers of cognition, yet the model layer is more concentrated than most physical inputs. Providers update models without notice sufficient to revalidate; retired versions may make past decisions irreproducible, defeating audit; and the same concentration that creates individual dependency creates sectoral correlation. Model providers belong in the supplier risk register with the treatment given to a sole-source supplier of a critical component, including documented alternatives, exit provisions, and tested fallback (Akin-Oluyomi et al., 2023b; Wedraogo et al., 2025).

3.3 The regulatory position

Table 4 summarizes the principal instruments as verified against official sources up to the July 2026 search cut-off stated in Section 2.2 (see also Section 2.4). Three observations follow.

Table 4. Governance instruments and allocation of responsibility

Instrument	Jurisdiction	Principal obligation	Locus of responsibility	Status
Regulation (EU) 2024/1689 (AI Act)	European Union	Risk management, data governance, logging, human oversight, transparency for high-risk systems	Provider and deployer	Transparency and literacy in force; high-risk obligations deferred to Dec. 2027 and Aug. 2028
Directive (EU) 2026/470 (CSDDD as amended)	European Union	Risk-based human rights and environmental due diligence across the chain of activities	In-scope undertaking	Scope narrowed; compliance deferred to 2029

Instrument	Jurisdiction	Principal obligation	Locus of responsibility	Status
UN Guiding Principles; OECD guidance	International	Identify and address adverse impacts caused or contributed to	Enterprise	Voluntary; incorporated by reference into binding regimes
ISO/IEC 42001	International	Certifiable AI management system	Deploying organisation	Voluntary; procurement-legible
NIST AI Risk Management Framework	United States	Govern, map, measure, and manage AI risk	Deploying organisation	Voluntary; contractually imposed
ISO 31000	International	Enterprise risk management architecture	Deploying organisation	Voluntary; integration backbone

The direction of travel is from voluntary guidance to binding obligation, but the timetable has moved. The European Union deferred high-risk obligations under its AI Regulation to December 2027 for standalone systems and August 2028 for embedded ones, while leaving transparency and AI literacy duties on their original schedule. Corporate sustainability due diligence was narrowed in scope and deferred to 2029, though negotiators rejected proposals to confine diligence to direct suppliers, so the risk-based approach still extends across the chain of activities. Readiness studies indicate that multinational enterprises are, on the whole, not positioned for either regime (European Parliament & Council of the European Union, 2024, 2026; Ominyi et al., 2024b).

Obligations attach to identifiable regulated entities while risk is generated by a distributed technical substrate. Regulation reaches the manufacturer or the in-scope undertaking; it does not reach the model provider whose update changed a decision boundary, nor the third-party data vendor whose error propagated into a supplier score. Comparable scope problems are documented across data protection regimes and platform liability frameworks (Ominyi & Anichukwueze, 2022a; Ominyi et al., 2025b).

Requirements are converging on transparency and diverging on verification. Instruments increasingly mandate disclosure of composition, logic, or impact; few mandate independent verification that the disclosure is accurate. Algorithmic accountability scholarship identifies this precisely. Transparency without the power to intervene produces no accountability (Ananny & Crawford, 2018); a general right to explanation of automated decisions is weaker than commonly assumed (Wachter et al., 2017); and trade secret protection is routinely invoked to limit what disclosure contains (Annan, 2024; Ominyi & Anichukwueze, 2023). Regulation is therefore reinforcing a coverage gap rather than closing it.

3.4 The Governed Autonomy Framework

The framework rests on six principles. Authority is granted rather than assumed. Accountability is assigned before deployment rather than attributed after an incident. Traceability is an operational requirement, not a documentation exercise. Transparency is calibrated to the audience, since regulators, boards, affected suppliers, and internal reviewers need different information at different depths. Contestability is the operative test of accountability. And resilience includes resilience to the AI layer itself, extending the redundancy, flexibility, and visibility levers of the resilience literature to the analytical layer that literature has treated as dependable infrastructure (Christopher & Peck, 2004; Ivanov & Dolgui, 2020; Sheffi & Rice, 2005; Wieland & Durach, 2021; Wu et al., 2025).

The framework comprises four layers ordered by dependency, with three cross-cutting enablers. Traceability is meaningless without a definition of what the system was authorised to do; assurance cannot proceed without a traceable record; and resilience measures cannot be specified without knowing which decisions are assured. Figure 2 shows the architecture, and Table 5 maps each mechanism from Table 3 to the layer that addresses it.

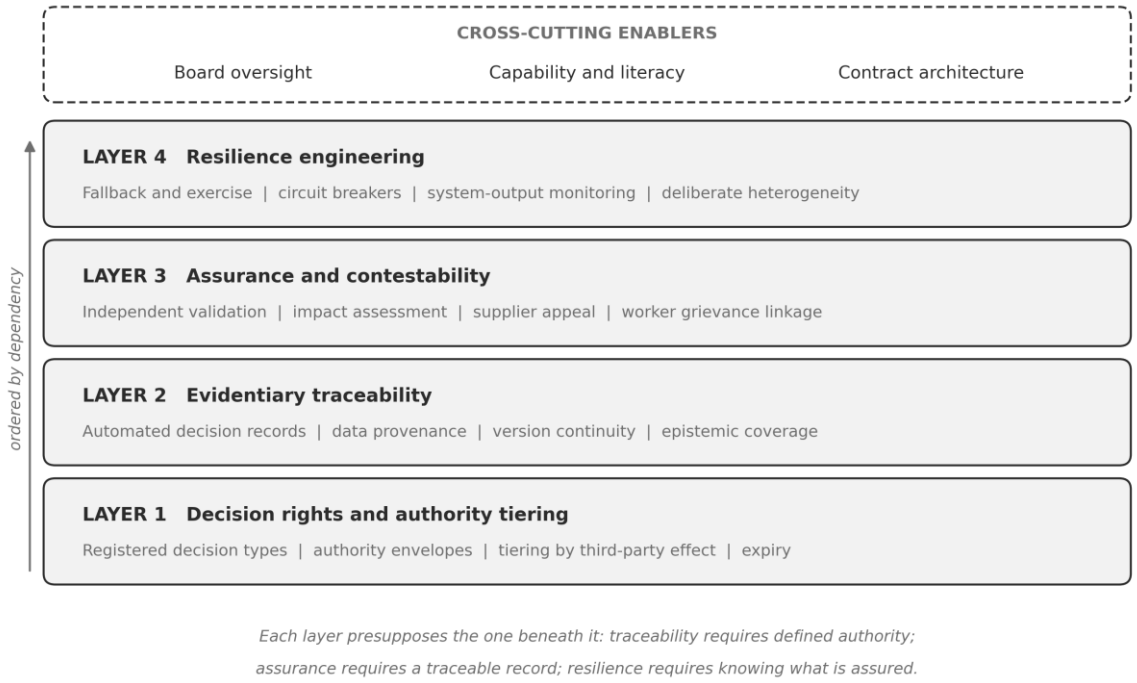


Figure 2. The Governed Autonomy Framework: four layers ordered by dependency, with cross-cutting enablers.

Table 5. Coverage of governance risk mechanisms by framework layer

Framework layer	M1	M2	M3	M4	M5	M6	M7
Layer 1: Decision rights and authority tiering	S	P		S	P	S	S
Layer 2: Evidentiary traceability	P	P	P		S	P	P
Layer 3: Assurance and contestability	P	S	S	S	P	S	S
Layer 4: Resilience engineering	S			P			P
Enabler: Board oversight	S	P	S	S	S	P	P
Enabler: Contract architecture		P	P	S	S	P	P

P = primary; S = supporting.

Layer 1: decision rights and authority tiering. Every AI-enabled decision type is registered with its configuration under Table 2, assigned by observed override rate rather than design intent. The registration records an authority envelope expressed as concrete limits on value, volume, counterparty class, geography, and duration; the named human authority who granted the delegation; the escalation trigger; the reversal mechanism and its latency; and an expiry date. Decision types are tiered by the severity and reversibility of their effect on parties outside the firm rather than by transaction value, so that a low-value automated decision terminating a small supplier's only customer relationship is treated as high tier. Decisions with irreversible third-party effects, including termination of a supplier relationship or designation as a sanctions or forced-labor risk, and any decision executed in a jurisdiction subject to heightened procurement compliance obligations (Okonkwo et al., 2021), remain advisory-only, with machine output entering as evidence in a documented human decision. Envelopes must be enforced technically rather than stated in policy, and multi-agent configurations require aggregate envelopes, because individually compliant agent actions can combine

into a commitment no single agent was authorised to make (Akanbi et al., 2025; Nwakamma et al., 2024b). Delegations expire and default to the prior tier unless positively renewed.

Layer 2: evidentiary traceability. For every registered decision the system persists an automated decision record. The record covers identifier and timestamp; decision type and tier; model or agent identity and exact version; configuration and thresholds in force; inputs with source and retrieval time; output including alternatives considered; the envelope invoked; whether human review occurred and with what result; the action executed; and links to any reversal or appeal. Reproducibility requires retention of model versions, or contractual commitments from vendors to retain retired versions for the applicable limitation period. Each data source carries a provenance record covering origin, licence, collection method, refresh frequency, coverage limitations, and personal data content with legal basis. Coverage limitation is the element most often omitted and most important: scores should carry an epistemic coverage indicator distinct from statistical confidence, because a low risk score with low coverage means the system found little where it examined little. The requirement is reviewability, meaning that the decision process as a whole rather than the model alone is recorded in a form permitting later scrutiny (Cobbe et al., 2021; Kroll et al., 2017), supported by artefact-level documentation of models and datasets (Gebru et al., 2021; Mitchell et al., 2019). Traceability infrastructure of this kind is already demonstrated through smart compliance and distributed-ledger audit trails (Abioye et al., 2023; Ekwunife et al., 2024) and in regulated-chain custody models (Aneke & Adesemoye, 2019; Eze et al., 2023).

Layer 3: assurance and contestability. Internal assurance follows a three-lines structure in which the deploying function owns performance, an independent function validates models and monitors envelope compliance, and internal audit examines whether tiering reflects observed behavior and whether reauthorization is substantive (Aliliele et al., 2025; Okojie, Filani, et al., 2023). Independent algorithmic audit and impact assessment provide the external counterpart (Metcalf et al., 2021; Raji et al., 2020; Selbst, 2021). Assessment is conducted before deployment and on material change, and must treat the objective function itself as an object of assessment, since a purchasing optimizer's effect on working hours is a property of what it maximizes rather than of how accurately it predicts.

Supplier contestability is the framework's principal departure from intra-organizational accountability models. Any supplier materially affected by a registered automated decision is entitled to five elements of process. These are notice that an automated system contributed materially, a statement of the principal factors at a level permitting meaningful response, a route to submit corrective information, review by a human with authority to reverse, and a determination within a stated period. Three objections arise. Confidentiality is answered by the fact that the entitlement is to principal factors rather than to the model. Volume is answered by restricting the entitlement to the two highest tiers. Gaming is answered by describing factor categories without exposing detection thresholds. The decisive justification is not ethical but epistemic. Suppliers hold information about themselves that no external data source contains, and they have a strong incentive to correct false positives; a firm that suppresses this channel is choosing to leave its own data quality defects undetected, and to participate in synchronized exit decisions that may be sector-wide errors. Supplier sustainability measurement research reports the same dependence on supplier-supplied data that no buyer-side system can reconstruct (Akin-Oluyomi, Okoruwa, et al., 2023).

Layer 4: resilience engineering. Each registered decision type requires a documented and periodically exercised fallback, since fallbacks that exist only on paper are not fallbacks. Because delegation erodes the skills that fallback presupposes, organizations must deliberately maintain the judgement, relationships, and category knowledge that resumption requires, which is a staffing and rotation question rather than a technology question (Essandoh et al., 2025). Circuit breakers limit the rate and aggregate scale of change an automated system can initiate, containing a data error rather than converting it into a supply crisis. Monitoring must cover the behavior of the decision system itself, including distribution shifts and divergence following a vendor model update (Nwakamma et al., 2024a; Ominyi et al., 2024a). Deliberate heterogeneity limits monoculture exposure by avoiding full dependence on a single model and data provider for critical decision classes and by reserving allocation weight for options a purely optimal solution would exclude. Resilience indices and diversification models from the supply chain literature supply the measurement apparatus

(Akinleye, 2024; Efobi et al., 2023; Ike et al., 2021; Ogunwole et al., 2021), and digital twin and ripple-effect methods provide a simulation environment in which fallback and propagation can be tested before they are needed (Ivanov et al., 2019; Kleindorfer & Saad, 2005; Sodhi & Tang, 2012).

Cross-cutting enablers. Board oversight requires periodic reporting of the registered inventory and tiers, delegations granted or renewed, incidents and reversals, override rates against expectation, supplier appeals and outcomes, vendor concentration, and fallback exercise results (Ike et al., 2024; Ominyi et al., 2026b). Capability is a precondition rather than a supplement, since category managers who cannot interrogate a score cannot discharge the oversight the framework assigns them. Contract architecture must transmit obligations both upstream and downstream. Upstream, contracts with vendors must cover disclosure of material model changes, revalidation rights, retention of retired versions, audit rights, incident notification, exit assistance, and liability allocation reflecting actual control. Downstream, contracts with suppliers must cover disclosure of automated decision-making, the contestability entitlement, and data correction obligations (Akin-Oluyomi et al., 2023b, 2024; Akinleye & Adeyoyin, 2022).

3.5 Operationalization

Table 6 presents a five-level maturity model. The gap that matters is between levels two and three, because level two produces documentation while level three produces control.

Table 6. Governance maturity for AI-enabled supply chain decisions

Level	Decision rights	Traceability	Assurance	Resilience
1. Ad hoc	Undocumented; authority emerges from configuration	Application logs only; decisions not reconstructable	None specific to AI	None; failure surfaces as operational incident
2. Defined	Inventory exists; tiers assigned by design intent	Decision records for high-consequence classes	Internal model validation	Documented fallback, untested
3. Controlled	Tiers assigned by observed behavior; envelopes enforced technically; delegations expire	Full records with provenance and version continuity	Independent validation; impact assessment; supplier appeal channel	Fallbacks exercised; circuit breakers; monitoring of system outputs
4. Assured	Board-level reauthorization; aggregate envelopes for multi-agent configurations	Reproducibility guaranteed contractually; epistemic coverage reported	External audit or certification; appeals analyzed as a quality signal	Deliberate heterogeneity; capability maintenance; scheduled manual operation
5. Adaptive	Authority adjusts to demonstrated performance under governance approval	Traceability extends across vendor and partner boundaries	Assurance results feed model and objective redesign	Sector-level coordination on correlated exposure

Governance performance requires measurement distinct from model performance. Authority integrity is measured by the proportion of decision types with current unexpired delegations, envelope breaches detected, and drift between designed and observed tier. Traceability is measured by the proportion of decisions with complete records, the proportion reproducible on demand, and median time to reconstruct a decision on request. Contestability is measured by supplier appeal rate, the proportion of appeals resulting in reversal, and median time to determination, noting that a reversal rate near zero suggests the channel is not functioning rather than that the system is faultless. Oversight effectiveness is measured by override rates against expectation and by whether overrides proved superior. Resilience is measured by time since last exercised fallback, concentration of critical decisions by provider, and vendor updates deployed without revalidation. Indicator frameworks of this type are established in performance governance practice (Babatope et al., 2023; Filani et al., 2023).

Implementation proceeds in four phases. The first inventories every AI-enabled decision type, including systems adopted by business functions without central visibility, classifies them by observed override rate, and stops any irreversible-effect decision currently executing without human authority. The second constructs the decision authority matrix and implements technical envelope enforcement and circuit breakers, which deliver the largest immediate risk

reduction per unit of effort. The third establishes independent validation and impact assessment, opens the supplier contestability channel, and renegotiates vendor contracts at renewal. The fourth pursues external assurance, addresses provider concentration, and integrates board reporting with due diligence governance ahead of the 2027 and 2029 regulatory dates.

4. Discussion

4.1 Trust transitivity and the limits of perimeter thinking

Every mechanism in Table 3 instantiates a single structural property: authority in automated supply chains is transitive and largely unverified. A firm makes an explicit decision about a small number of systems and thereby inherits, without further decision, the design choices of every model provider, data vendor, and configuration author upstream of them. Perimeter-derived controls underperform here because they assume a boundary across which trust is granted and can be withheld, whereas a decision pipeline offers only a gradient of decreasing visibility. The properties that matter are therefore verifiability properties rather than access-control properties, which is the same conclusion reached in the procedural regularity literature on accountable algorithms (Cobbe et al., 2021; Kroll et al., 2017).

4.2 Transparency without verification

The regulatory and research emphasis on disclosure is not misplaced but is incomplete in a diagnosable way. Disclosure of composition, logic, or impact and verification of provenance and behavior answer different questions, and only the second detects the failure that dominates practice: a system operating exactly as specified on inputs that were wrong, or optimizing exactly the objective it was given with consequences nobody assessed. The corpus contains mature instruments for verification, including independent validation, impact assessment, and audit trail architecture (Abioye et al., 2023; Okojie, Filani, et al., 2023; Ominyi et al., 2026b), and shows them under-adopted while disclosure absorbs the compliance budget. Closing that gap is the highest-value near-term intervention available to practitioners and standards bodies alike. Firms that treat verifiable governance as a market signal rather than as a cost report competitive benefit from it (Annan, 2025b).

4.3 The temporal argument

Machine decision cycles are measured in seconds and minutes; governance cycles in weeks and quarters. Quarterly supplier review, annual model validation, and periodic audit are correctly designed for a decision rate that no longer obtains. Two implications follow. Controls should be repositioned from periodic to synchronous, meaning enforcement at the point of decision through envelopes and circuit breakers rather than review after the fact. And latency should be introduced deliberately for high-consequence decision classes, so that reversal remains possible within the window in which harm can still be undone.

4.4 Artificial intelligence on both sides of the problem

AI enters the analysis in three roles that are frequently conflated, and conflating them produces confused conclusions. As a source of exposure it introduces opacity, monoculture, and displaced coercion. As an instrument of control it enables continuous compliance monitoring, anomaly detection, and automated assurance at volumes human review cannot approach (Ominyi et al., 2024a, 2025a). And as an object of governance it requires the approval, documentation, and audit obligations that regulated industries already apply to models treated as production assets (Ominyi & Anichukwueze, 2023, 2024; Ominyi et al., 2026a). Automated release-gating of model behavior offers a control point that transfers directly to supply chain deployment (Nwakamma et al., 2024a). Agentic systems separately introduce a distinct threat class comprising prompt injection, tool poisoning, memory manipulation, and excessive agency, which must be governed at the point of tool access rather than at the point of output (Nwakamma et al., 2024b). Data curation practice determines much of what a deployed system will do, which places provenance discipline upstream of model governance rather than beside it (Oyesiji et al., 2024).

4.5 Incentives and the location of marginal return

Regulatory obligations and compliance budgets sit with the buying organization. The exposures that matter most, including deep-tier opacity and displaced coercion, are generated where that organization has least visibility and least contractual reach. This suggests that the implicit model, in which governance is procured downstream and enforced by audit, is misaligned with where the marginal return is highest. Mechanisms that invest upstream, including supplier capability development, data quality collaboration, and relationship structures that make disclosure rational for the supplier, target the actual point of failure (Akin-Oluyomi et al., 2024; Akinleye & Adeyoyin, 2022; Efobi et al., 2022; Ike et al., 2021). Sustainable and green procurement research reaches a compatible conclusion, finding that supplier-side capability rather than buyer-side specification determines whether standards are met in practice (Akin-Oluyomi et al., 2023a; Akinleye et al., 2023; Okojie et al., 2020). The corpus contains little evaluation of such mechanisms against downstream governance outcomes, which is the principal research gap.

4.6 Limitations

The framework is conceptual and has not been empirically validated; its costs and effectiveness in operation are unknown. Full implementation will be feasible primarily for large firms, which risks a governance gap in which mid-sized enterprises deploy comparable systems without comparable controls, and a competitive dynamic in which governance becomes a disadvantage. Supplier contestability is the least tested element, and whether it functions at scale in networks of tens of thousands of suppliers is an open empirical question. Much of the framework depends on contractual leverage that firms may not possess against concentrated model providers. The regulatory analysis reflects instrument texts and amendments as verified against official sources up to the July 2026 search cut-off (Section 2.2, Section 2.4), a period of active amendment; readers relying on this account for compliance purposes should verify current requirements against the primary regulatory texts rather than against this account. And the monoculture problem exceeds the framework, since firm-level measures reduce a firm's contribution and vulnerability but cannot resolve what is fundamentally a collective action problem.

4.7 Research agenda

Six directions follow. Measurement of correlation, establishing the degree of model and data overlap across firms within sectors and the extent to which supplier screening outcomes actually converge. Field evaluation of contestability, covering usage, reversal rates, effects on data quality, and administrative cost. Treatment of objective functions as objects of due diligence, including constraint formulations that embed labor standards in the optimization rather than in downstream monitoring (Ike et al., 2022; Nnabueze et al., 2023). Extension of human oversight research to supply chain settings, examining the conditions under which override authority is genuinely exercised (Ladapo et al., 2022, 2024). Methods for quantifying and communicating epistemic coverage in poorly observed regions of supplier networks (Okojie, Ike, et al., 2023). And formal treatment of aggregate envelope enforcement where multiple agents can combine compliant actions into an unauthorized aggregate commitment (Akanbi et al., 2025; Ogundairo, 2025).

5. Conclusion

The delegation of supply chain decisions to machines is proceeding faster than the construction of the institutions needed to answer for them. This is not principally a technical failure, since the models are in many applications better than the human judgement they replace. The failure is institutional. Authority migrates without being granted; records adequate to reconstruct decisions are not kept; the parties best placed to detect errors have no route to report them; and the correlated risk created by a whole sector reasoning with the same tools appears on no firm's risk register.

The review advances four claims. Accountability structures rarely track the actual locus of decision, and advisory systems with high acceptance rates should be governed as delegated ones. Seven distinct mechanisms generate governance risk, of which algorithmic monoculture and displaced coercion are the least addressed in current practice.

A framework adequate to the problem must grant authority explicitly and bound it technically, record decisions in reconstructable form, extend assurance to the affected parties, and treat the AI layer itself as a source of exposure. And supplier contestability is the most valuable and most neglected control available, justified less by fairness than by the fact that the supplier holds information the model cannot otherwise obtain.

Two practical conclusions follow. Human oversight is not a control unless the reviewer has the time, information, capability, and authority to override, and unless the organization measures whether overrides occur; declared oversight that does not function is worse than acknowledged automation, because it supplies false assurance. And current regulatory deferrals are not grounds for delay, because the evidentiary record that later compliance will require has to be created contemporaneously. The question facing governing bodies is not whether to permit machine decision-making in their supply chains, which is settled in practice, but whether they will be able to account for what those machines do. That capacity is built deliberately and in advance, or it is unavailable when it is needed.

Author Contributions

All authors contributed equally to the conceptualization of the article and writing of the original and subsequent drafts. All authors have read and agreed to the published version of the manuscript.

Data Availability Statement

Not applicable. This review did not generate or analyse new datasets; all sources analyzed are listed in the References.

Acknowledgements

Not applicable.

Ethical considerations

The authors avoided data fabrication, falsification, and plagiarism, and any form of misconduct. The study did not involve human participants or animals, so ethical approval was not required.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Conflict of interest

The authors declare no conflict of interest.

References

Abioye, R. F., Okojie, J. S., Filani, O. M., Ike, P. N., Idu, J. O. O., Nnabueze, S. B., Okojokwu-Idu, J. O., & Ihwughwavwe, S. I. (2023). Automated ESG reporting in energy projects using blockchain-driven smart compliance management systems. *International Journal of Multidisciplinary Evolutionary Research, 4*(2), 120–129. https://doi.org/10.54660/IJMER.2023.4.2.120-129

Agbabiaka, J., Okonkwo, C. S., Ogunwole, O., Mayo, W., & Okeke, O. T. (2019). Supply chain risk management model for EPC and gas processing projects. *Iconic Research and Engineering Journals, 3*(2), 968–980. https://doi.org/10.64388/IREV3I2-1713124

Ahiaeke Patrick, M. C., Okonkwo, C. S., Mayo, W., & Okeke, O. T. (2021). Model for data driven vendor evaluation and bid selection using geospatial intelligence. *Shodhshauryam, International Scientific Refereed Research Journal, 4*(4), 426–443. https://doi.org/10.32628/SHISRRJ214461

Aifuwa, S. E., Oshoba, T. O., Ogbuefi, E., Ike, P. N., Nnabueze, S. B., & Olatunde-Thorpe, J. (2020). Predictive analytics models enhancing supply chain demand forecasting accuracy and reducing inventory management inefficiencies. *International Journal of Multidisciplinary Research and Growth Evaluation, 1*(3), 171–181. https://doi.org/10.54660/.IJMRGE.2020.1.3.171-181

Akanbi, O., Ganiu, O. S., & Sunday, E. A. (2025). A multi-agent AI framework for swarm intelligence in autonomous mobile robot (AMR) fleet coordination. *International Journal of Scientific Research in Humanities and Social Sciences, 2*(1), 81–109.

Akanbi, O., & Sunday, E. A. (2024). An integrated path-planning and slotting optimization model for AMR-enabled high-density warehousing. *International Journal of Advanced Multidisciplinary Research and Studies, 4*(6), 3226–3243. https://doi.org/10.62225/2583049X.2024.4.6.6181

Akanbi, O., & Sunday, E. A. (2025). A systematic review of AI-driven autonomous mobile robots (AMR) in scalable micro-fulfillment centers. *International Journal of Advanced Multidisciplinary Research and Studies, 5*(6), 2363–2379. https://doi.org/10.62225/2583049X.2025.5.6.6182

Akin-Oluyomi, O. T., Atima, M. E., & Akinleye, O. K. (2023a). Green procurement strategies for balancing cost efficiency with long-term environmental responsibility. *International Journal of Advanced Multidisciplinary Research and Studies, 3*(6), 2183–2193.

Akin-Oluyomi, O. T., Atima, M. E., & Akinleye, O. K. (2023b). Regulatory compliance and supplier risk assessment frameworks in international pharmaceutical procurement. *International Journal of Advanced Multidisciplinary Research and Studies, 3*(6), 2194–2204.

Akin-Oluyomi, O. T., Atima, M. E., & Akinleye, O. K. (2024). Cross-border supplier relationship management frameworks for pharmaceutical and global construction sectors. *International Journal of Multidisciplinary Research and Growth Evaluation, 5*(6), 1709–1718.

Akin-Oluyomi, O. T., Atima, M. E., Akinleye, O. K., & Okoruwa, P. O. (2023). Predictive analytics approaches for improving demand forecasting accuracy in e-commerce procurement systems. *International Journal of Advanced Multidisciplinary Research and Studies, 3*(6), 2173–2182.

Akin-Oluyomi, O. T., Okoruwa, P. O., Babatope, O. M., & Akokodaripon, D. A. (2023). Evaluating supplier sustainability metrics through data-driven procurement and supply chain frameworks. *International Journal of Advanced Multidisciplinary Research and Studies, 3*(6), 2213–2223.

Akinlade, O. F., Filani, O. M., & Nwachukwu, P. S. (2024). Automation and digital twins framework reducing procurement errors and turnaround time. *International Journal of Scientific Research in Humanities and Social Sciences, 1*(1), 197–216.

Akinleye, O. K. (2024). A sustainable procurement and resilience framework for post-pandemic pharmaceutical operations. *International Journal of Advanced Multidisciplinary Research and Studies, 4*(1), 1602–1621.

Akinleye, O. K., & Adeyoyin, O. (2021). Process automation framework for enhancing procurement efficiency and transparency. *Shodhshauryam, International Scientific Refereed Research Journal, 4*(4), 356–387.

Akinleye, O. K., & Adeyoyin, O. (2022). Supplier relationship management framework for achieving strategic procurement objectives. *Gyanshauryam, International Scientific Refereed Research Journal, 5*(4), 565–598. https://doi.org/10.32628/GISRRJ225430

Akinleye, O. K., Okoruwa, P. O., Babatope, O. M., & Akokodaripon, D. A. (2023). Leveraging big data and business intelligence for optimization of manufacturing sector procurement. *International Journal of Advanced Multidisciplinary Research and Studies, 3*(6), 2164–2172.

Aliliele, C., Mbonu, I. S., Uzoka, E., & Iwuanyanwu, U. (2025). A review of AI assisted continuous auditing systems in technology risk and cybersecurity oversight. *Gyanshauryam, International Scientific Refereed Research Journal, 8*(4), 210–250. https://doi.org/10.32628/GISRRJ258369

Ananny, M., & Crawford, K. (2018). Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. *New Media & Society, 20*(3), 973–989. https://doi.org/10.1177/1461444816676645

Aneke, O. B., & Adesemoye, A. C. (2019). Toward an integrated conceptual framework for traceability and chain-of-custody integrity in pharmaceutical distribution. *Iconic Research and Engineering Journals, 3*(4), 655–672.

Aneke, O. B., Sydney, E., & Adesemoye, A. C. (2023). Data integrity and governance in regulated life sciences operations: A review of failures, controls, and remediation strategies. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 9*(10), 538–568.

Annan, A. O. (2022). Data privacy governance models for cross-border digital platforms. *International Journal of Multidisciplinary Research and Growth Evaluation, 3*(6), 949–964.

Annan, A. O. (2024). Algorithmic accountability and trade secret protection in artificial intelligence. *Shodhshauryam, International Scientific Refereed Research Journal, 7*(5), 315–347.

Annan, A. O. (2025a). Automated decision-making and anti-discrimination compliance under U.S. law. *International Journal of Advanced Multidisciplinary Research and Studies, 5*(2), 2522–2540.

Annan, A. O. (2025b). Cybersecurity compliance as a source of competitive advantage in technology markets. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 11*(5), 456–487.

Babatope, O. M., Akokodaripon, D. A., Akinleye, O. K., & Okoruwa, P. O. (2023). The role of data visualization in enhancing strategic procurement decision-making effectiveness. *International Journal of Advanced Multidisciplinary Research and Studies, 3*(6), 2205–2212.

Baryannis, G., Validi, S., Dani, S., & Antoniou, G. (2019). Supply chain risk management and artificial intelligence: State of the art and future research directions. *International Journal of Production Research, 57*(7), 2179–2202. https://doi.org/10.1080/00207543.2018.1530476

Bovens, M. (2007). Analysing and assessing accountability: A conceptual framework. *European Law Journal, 13*(4), 447–468. https://doi.org/10.1111/j.1468-0386.2007.00378.x

Burrell, J. (2016). How the machine thinks: Understanding opacity in machine learning algorithms. *Big Data & Society, 3*(1), 1–12. https://doi.org/10.1177/2053951715622512

Choi, T.-M., Wallace, S. W., & Wang, Y. (2018). Big data analytics in operations management. *Production and Operations Management, 27*(10), 1868–1883. https://doi.org/10.1111/poms.12838

Christopher, M., & Peck, H. (2004). Building the resilient supply chain. *The International Journal of Logistics Management, 15*(2), 1–14. https://doi.org/10.1108/09574090410700275

Cobbe, J., Lee, M. S. A., & Singh, J. (2021). Reviewable automated decision-making: A framework for accountable algorithmic systems. In *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency* (pp. 598–609). ACM. https://doi.org/10.1145/3442188.3445921

Danielsson, J., Macrae, R., & Uthemann, A. (2022). Artificial intelligence and systemic risk. *Journal of Banking & Finance, 140*, Article 106290. https://doi.org/10.1016/j.jbankfin.2021.106290

Diakopoulos, N. (2016). Accountability in algorithmic decision making. *Communications of the ACM, 59*(2), 56–62. https://doi.org/10.1145/2844110

Efobi, O. Z., Akinleye, O. K., & Fasawe, O. (2022). Conceptual model for data-driven lean supply chain optimization in manufacturing and retail operations. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 8*(2), 703–734. https://doi.org/10.32628/CSEIT2541335

Efobi, O. Z., Akinleye, O. K., & Fasawe, O. (2023). Conceptual framework for developing a resilience index for post-pandemic supply chains. *Shodhshauryam, International Scientific Refereed Research Journal, 6*(2), 421–432.

Ekwunife, D. I., Precious, O. T., Rasul, O. A., Akinlade, O. F., Nwokoro, T. O., & Ikpe, V. I. (2024). Using blockchain technology to maximize supply chain and logistics management in North America. *International Journal of Science and Research Archive, 12*(2), 854–863.

Elish, M. C. (2019). Moral crumple zones: Cautionary tales in human-robot interaction. *Engaging Science, Technology, and Society, 5*, 40–60. https://doi.org/10.17351/ests2019.260

Essandoh, S., Sakyi, J. K., Ibrahim, A. K., Okafor, C. M., & Wedraogo, L. (2025). Artificial intelligence and the future of work: Impacts on employment and job roles. *International Journal of Multidisciplinary Futuristic Development, 6*(1), 31–41. https://doi.org/10.54660/IJMFD.2025.6.1.31-41

European Parliament & Council of the European Union. (2024). *Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. Official Journal of the European Union, L 2024/1689. http://data.europa.eu/eli/reg/2024/1689/oj

European Parliament & Council of the European Union. (2026). *Directive (EU) 2026/470 amending Directives 2013/34/EU, 2006/43/EC, (EU) 2022/2464 and (EU) 2024/1760 as regards corporate sustainability reporting and due diligence requirements*. Official Journal of the European Union.

Eze, F. I., Anene, U. N., & Akinleye, O. K. (2023). Pharmaceutical supply chain governance, environmental risk management, and sustainable access to essential medicines in emerging economies: The PSCG-ERM framework. *International Journal of Health and Pharmaceutical Research, 8*(4), 192–241. https://doi.org/10.56201/ijhpr.v8.no4.2023.pg192.241

Filani, O. M., Nnabueze, S. B., Ike, P. N., & Wedraogo, L. (2022). Real-time risk assessment dashboards using machine learning in hospital supply chain management systems. *International Journal of Multidisciplinary Evolutionary Research, 3*(1), 65–76. https://doi.org/10.54660/IJMER.2022.3.1.65-76

Filani, O. M., Nnabueze, S. B., Sakyi, J. K., & Okojie, J. S. (2023). Scenario-based financial modelling for enhancing strategic decision-making and organizational long-term planning. *Journal of Frontiers in Multidisciplinary Research, 4*(2), 251–265. https://doi.org/10.54660/.JFMR.2023.4.2.251-265

Gebru, T., Morgenstern, J., Vecchione, B., Vaughan, J. W., Wallach, H., Daumé III, H., & Crawford, K. (2021). Datasheets for datasets. *Communications of the ACM, 64*(12), 86–92. https://doi.org/10.1145/3458723

Green, B. (2022). The flaws of policies requiring human oversight of government algorithms. *Computer Law & Security Review, 45*, Article 105681. https://doi.org/10.1016/j.clsr.2022.105681

Green, B., & Chen, Y. (2019). The principles and limits of algorithm-in-the-loop decision making. *Proceedings of the ACM on Human-Computer Interaction, 3*(CSCW), Article 50. https://doi.org/10.1145/3359152

Huertos, F. J., Bañales, O., Alvarez, P., & Cabanes, I. (2026). Multi-agent reinforcement learning for cooperative manipulation in industrial robotics: A systematic review of trends, gaps and research drivers. *Robotics, 15*(8), Article 156. https://doi.org/10.3390/robotics15080156

Ike, P. N., Aifuwa, S. E., Nnabueze, S. B., Olatunde-Thorpe, J., Ogbuefi, E., Oshoba, T. O., & Akokodaripon, D. (2024). Quantitative risk architecture for public-private partnerships: A multi-layered model for allocating public and private risk. *International Journal of Advanced Multidisciplinary Research and Studies, 4*(6), 2669–2682. https://doi.org/10.62225/2583049X.2024.4.6.5021

Ike, P. N., Ogbuefi, E., Nnabueze, S. B., Olatunde-Thorpe, J., Aifuwa, S. E., Oshoba, T. O., & Akokodaripon, D. (2021). Supplier relationship management strategies fostering innovation, collaboration, and resilience in global supply chain ecosystems. *International Journal of Multidisciplinary Evolutionary Research, 2*(2), 52–62. https://doi.org/10.54660/IJMER.2021.2.2.52-62

Ike, P. N., Ogbuefi, E., Nnabueze, S. B., Olatunde-Thorpe, J., Aifuwa, S. E., Oshoba, T. O., & Akokodaripon, D. (2022). Lean supply chain practices improving operational efficiency, reducing waste, and enhancing organizational competitiveness globally. *Journal of Frontiers in Multidisciplinary Research, 3*(2), 182–192. https://doi.org/10.54660/.IJFMR.2022.3.2.182-192

International Organization for Standardization. (2018). *Risk management: Guidelines* (ISO Standard No. 31000:2018). ISO. https://www.iso.org/standard/65694.html

International Organization for Standardization & International Electrotechnical Commission. (2023). *Information technology: Artificial intelligence: Management system* (ISO/IEC Standard No. 42001:2023). ISO/IEC. https://www.iso.org/standard/81230.html

Ivanov, D., & Dolgui, A. (2020). Viability of intertwined supply networks: Extending the supply chain resilience angles towards survivability. A position paper motivated by COVID-19 outbreak. *International Journal of Production Research, 58*(10), 2904–2915. https://doi.org/10.1080/00207543.2020.1750727

Ivanov, D., Dolgui, A., & Sokolov, B. (2019). The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics. *International Journal of Production Research, 57*(3), 829–846. https://doi.org/10.1080/00207543.2018.1488086

Kim, Y., Chen, Y.-S., & Linderman, K. (2015). Supply network disruption and resilience: A network structural perspective. *Journal of Operations Management, 33–34*, 43–59. https://doi.org/10.1016/j.jom.2014.10.006

Kleinberg, J., & Raghavan, M. (2021). Algorithmic monoculture and social welfare. *Proceedings of the National Academy of Sciences, 118*(22), Article e2018340118. https://doi.org/10.1073/pnas.2018340118

Kleindorfer, P. R., & Saad, G. H. (2005). Managing disruption risks in supply chains. *Production and Operations Management, 14*(1), 53–68. https://doi.org/10.1111/j.1937-5956.2005.tb00009.x

Kroll, J. A., Huey, J., Barocas, S., Felten, E. W., Reidenberg, J. R., Robinson, D. G., & Yu, H. (2017). Accountable algorithms. *University of Pennsylvania Law Review, 165*(3), 633–705. https://scholarship.law.upenn.edu/penn_law_review/vol165/iss3/3

Kumar, R. J., Kumar, I. A., Eswaran, M., Mohan, M. B., Aseer, R. J., & Bahubalendruni, M. V. A. R. (2026). Autonomous mobile robots in intelligent warehousing: Workflow-centric integration for Industry 5.0 logistics. *Advanced Engineering Informatics, 76*(Part A), Article 104858. https://doi.org/10.1016/j.aei.2026.104858

Ladapo, O. O., Dosunmu, A. A., Jooda, D., & Abolaji, T. O. (2022). Human-in-the-loop machine learning: A state of the art. *Journal of Frontiers in Multidisciplinary Research, 3*(1), 656–669. https://doi.org/10.54660/.JFMR.2022.3.1.656-669

Ladapo, O. O., Jooda, D., Dosunmu, A. A., & Abolaji, T. O. (2024). Keeping humans in the loop: Human-centered automated annotation with generative AI. *International Journal of Multidisciplinary Futuristic Development, 5*(1), 81–95. https://doi.org/10.54660/IJMFD.2024.5.1.81-95

LeBaron, G., & Lister, J. (2015). Benchmarking global supply chains: The power of the ethical audit regime. *Review of International Studies, 41*(5), 905–924. https://doi.org/10.1017/S0260210515000388

Locke, R. M. (2013). *The promise and limits of private power: Promoting labor standards in a global economy*. Cambridge University Press. https://doi.org/10.1017/CBO9781139381840

Metcalf, J., Moss, E., Watkins, E. A., Singh, R., & Elish, M. C. (2021). Algorithmic impact assessments and accountability: The co-construction of impacts. In *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency* (pp. 735–746). ACM. https://doi.org/10.1145/3442188.3445935

Mitchell, M., Wu, S., Zaldivar, A., Barnes, P., Vasserman, L., Hutchinson, B., Spitzer, E., Raji, I. D., & Gebru, T. (2019). Model cards for model reporting. In *Proceedings of the Conference on Fairness, Accountability, and Transparency* (pp. 220–229). ACM. https://doi.org/10.1145/3287560.3287596

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society, 3*(2), 1–21. https://doi.org/10.1177/2053951716679679

National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)* (NIST AI 100-1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.100-1

Nissenbaum, H. (1996). Accountability in a computerized society. *Science and Engineering Ethics, 2*(1), 25–42. https://doi.org/10.1007/BF02639315

Nnabueze, S. B., Filani, O. M., Sakyi, J. K., Okojie, J. S., & Okereke, M. (2023). Developing sustainable business models for large-scale service organizations using predictive and strategic insights. *International Journal of Multidisciplinary Evolutionary Research, 4*(2), 76–88. https://doi.org/10.54660/IJMER.2023.4.2.76-88

Nnabueze, S. B., Ike, P. N., Olatunde-Thorpe, J., Aifuwa, S. E., Oshoba, T. O., Ogbuefi, E., & Akokodaripon, D. (2021). End-to-end visibility frameworks improving transparency, compliance, and traceability across complex global supply chain operations. *International Journal of Multidisciplinary Futuristic Development, 2*(2), 50–60. https://doi.org/10.54660/IJMFD.2021.2.2.50-60

Nwakamma, S., Ojukwu, J., & Oyesiji, S. O. (2024a). LLM-as-a-judge for automated model governance: A review of methods, biases, and release-gating practices. *World Journal of Innovation and Modern Technology, 8*(6), 185–216. https://doi.org/10.56201/wjimt.v8.no6.2024.pg185.216

Nwakamma, S., Ojukwu, J., & Oyesiji, S. O. (2024b). Securing agentic AI enterprise workflows against prompt injection, tool poisoning, memory manipulation, and excessive agency threats. *World Journal of Innovation and Modern Technology, 8*(6), 217–248. https://doi.org/10.56201/wjimt.v8.no6.2024.pg217.248

Ogundairo, K. M. (2025). Hardening the autonomous value chain: Lean Six Sigma guardrails and multi-enterprise ETL architecture for agentic supply chain orchestration. *IIARD International Journal of Economics and Business Management, 11*(12), 441–478. https://doi.org/10.56201/ijebm.vol.11.no12.2025.pg441.478

Ogunwole, O., Okonkwo, C. S., Agbabiaka, J., Mayo, W., & Okeke, O. T. (2021). Supply chain resilience framework for critical infrastructure and gas processing plants. *Shodhshauryam, International Scientific Refereed Research Journal, 4*(4), 444–461. https://doi.org/10.32628/SHISRRJ214462

Okojie, J., Ike, P., Idu, J., Nnabueze, S. B., Filani, O., & Ihwughwavwe, S. (2023). Predictive analytics models for monitoring smart city emissions and infrastructure risk in urban ESG planning. *International Journal of Multidisciplinary Futuristic Development, 4*(1), 45–57. https://doi.org/10.54660/IJMFD.2023.4.1.45-57

Okojie, J. S., Filani, O. M., Ihwughwavwe, S. I., & Sakyi, J. K. (2020). Sustainable procurement practices: ESG-integrated supply chain models for corporate responsibility and environmental performance. *Iconic Research and Engineering Journals, 4*(2).

Okojie, J. S., Filani, O. M., Ike, P. N., Okojokwu-Idu, J. O., Nnabueze, S. B., & Ihwughwavwe, S. I. (2023). Integrating AI with ESG metrics in smart infrastructure auditing for high-impact urban development projects. *International Journal of Multidisciplinary Futuristic Development, 4*(1), 32–44. https://doi.org/10.54660/IJMFD.2023.4.1.32-44

Okonkwo, C. S., Agbabiaka, J., Mayo, W., & Okeke, O. T. (2024a). Conceptual framework for digital supply chain governance in energy and infrastructure sectors. *Gyanshauryam, International Scientific Refereed Research Journal, 7*(4), 335–356. https://doi.org/10.32628/GISRRJ247423

Okonkwo, C. S., Agbabiaka, J., Mayo, W., & Okeke, O. T. (2024b). Framework for secure and scalable supply chain systems supporting national energy reliability. *International Journal of Advanced Multidisciplinary Research and Studies, 4*(6), 2816–2826. https://doi.org/10.62225/2583049X.2024.4.6.5494

Okonkwo, C. S., Agbabiaka, J., Mayo, W., & Okeke, O. T. (2024c). Model for predictive procurement planning to sustain operational uptime. *International Journal of Scientific Research in Humanities and Social Sciences, 1*(2), 909–928. https://doi.org/10.32628/IJSRSSH242772

Okonkwo, C. S., Agbabiaka, J., Mayo, W., & Okeke, O. T. (2024d). Review of advances in procurement strategy, ERP adoption, and logistics performance. *International Journal of Advanced Multidisciplinary Research and Studies, 4*(6), 2827–2835. https://doi.org/10.62225/2583049X.2024.4.6.5495

Okonkwo, C. S., Agbabiaka, J., Mayo, W., & Okeke, O. T. (2024e). Review of digital supply chain models for cost control and operational continuity. *International Journal of Advanced Multidisciplinary Research and Studies, 4*(6), 2836–2846. https://doi.org/10.62225/2583049X.2024.4.6.5496

Okonkwo, C. S., Agbabiaka, J., Mayo, W., & Okeke, O. T. (2024f). Supply chain automation framework using service management platforms. *Shodhshauryam, International Scientific Refereed Research Journal, 7*(2), 157–177. https://doi.org/10.32628/SHISRRJ2472157

Okonkwo, C. S., Agbabiaka, J., Okeke, O. T., & Mayo, W. (2025). Framework for national-scale supply chain optimization through integrated IT and procurement systems. *Gulf Journal of Advance Business Research, 3*(12), 1610–1625. https://doi.org/10.51594/gjabr.v3i12.189

Okonkwo, C. S., Ahiaeke Patrick, M. C., Okeke, O. T., & Mayo, W. (2023). Framework for integrating IT systems engineering with supply chain operations. *International Journal of Advanced Multidisciplinary Research and Studies, 3*(6), 2580–2589. https://doi.org/10.62225/2583049X.2023.3.6.5500

Okonkwo, C. S., Ogunwole, O., Mayo, W., & Okeke, O. T. (2021). Framework for regulatory-compliant procurement in high-risk energy environments. *International Journal of Multidisciplinary Research and Growth Evaluation, 2*(6), 595–605. https://doi.org/10.54660/IJMRGE.2021.2.6.595-605

Okoruwa, P. O., Babatope, O. M., Akokodaripon, D. A., & Akinleye, O. K. (2024). Developing integrated digital platforms for enhancing transparency in procurement and supply chain management. *International Journal of Multidisciplinary Research and Growth Evaluation, 5*(6), 1719–1729.

Okoruwa, P. O., Babatope, O. M., Akokodaripon, D. A., & Akinleye, O. K. (2025). Digital procurement transformation approaches for strengthening efficiency in global supply chain management. *International Journal of Multidisciplinary Research and Growth Evaluation, 6*(5), 975–985.

Ominyi, M., & Anichukwueze, C. C. (2022a). A conceptual framework for harmonizing data protection compliance across GDPR, NDPR, and United States privacy regimes. *International Journal of Social Sciences and Management Research, 8*(5), 148–174. https://doi.org/10.56201/ijssmr.v8.no5.2022.pg148.174

Ominyi, M., & Anichukwueze, C. C. (2022b). Reviewing greenhouse gas disclosure and ESG compliance obligations for energy and infrastructure enterprises under evolving regulatory regimes. *International Journal of Economics and Financial Management, 7*(6), 94–124. https://doi.org/10.56201/ijefm.v7.no6.2022.pg94.124

Ominyi, M., & Anichukwueze, C. C. (2023). A review of algorithmic accountability and model risk management approaches in financial services. *Journal of Accounting and Financial Management, 9*(12), 218–238. https://doi.org/10.56201/jafm.v9.no12.2023.pg218.238

Ominyi, M., & Anichukwueze, C. C. (2024). Conceptualizing responsible AI governance structures for automated decision systems in regulated industries. *International Journal of Social Sciences and Management Research, 10*(11), 403–430. https://doi.org/10.56201/ijssmr.v10.no11.2024.pg.403.430

Ominyi, M., Anichukwueze, C. C., & Uzougbo, N. S. (2024a). Developing a conceptual framework for AI-assisted compliance monitoring and anomaly detection in high-volume transaction environments. *World Journal of Innovation and Modern Technology, 8*(6), 204–228. https://doi.org/10.56201/wjimt.v8.no6.2024.pg204.228

Ominyi, M., Anichukwueze, C. C., & Uzougbo, N. S. (2024b). A systematic review of organizational readiness for the EU Artificial Intelligence Act in multinational enterprises. *World Journal of Innovation and Modern Technology, 8*(6), 185–203. https://doi.org/10.56201/wjimt.v8.no6.2024.pg185.203

Ominyi, M., Anichukwueze, C. C., & Uzougbo, N. S. (2025a). A conceptual framework for multi-agent AI quality control in the review of regulated documents. *International Journal of Social Sciences and Management Research, 11*(8), 534–557. https://doi.org/10.56201/ijssmr.vol.11no8.2025.pg534.557

Ominyi, M., Anichukwueze, C. C., & Uzougbo, N. S. (2025b). A review of intermediary liability and content governance obligations for digital platforms under the DSA, DMCA, and CDA regimes. *International Journal of Social Sciences and Management Research, 11*(8), 558–582. https://doi.org/10.56201/ijssmr.vol.11no8.2025.pg558.582

Ominyi, M., Anichukwueze, C. C., & Uzougbo, N. S. (2025c). Reviewing legal privilege and confidentiality challenges in enterprise deployment of large language models. *Journal of Law and Global Policy, 10*(3), 150–176. https://doi.org/10.56201/jlgp.vol.10.no3.2025.pg150.176

Ominyi, M., Anichukwueze, C. C., & Uzougbo, N. S. (2026a). A conceptual model for integrating legal, quantitative, and operational disciplines in next-generation regulatory risk leadership. *International Journal*

of Social Sciences and Management Research, 12(7), 524–550. https://doi.org/10.56201/ijssmr.vol.12no7.2026.pg524.550

Ominyi, M., Anichukwueze, C. C., & Uzougbo, N. S. (2026b). Conceptualizing enterprise AI governance functions as institutional standards for auditable and defensible risk management. *Journal of Accounting and Financial Management, 12*(7), 326–356. https://doi.org/10.56201/jafm.vol.12.no7.2026.p326.356

Organisation for Economic Co-operation and Development. (2018). *OECD due diligence guidance for responsible business conduct*. OECD Publishing.

Organisation for Economic Co-operation and Development. (2023). *OECD guidelines for multinational enterprises on responsible business conduct*. OECD Publishing. https://doi.org/10.1787/81f92357-en

Oyesiji, S. O., Nwakamma, S., & Ojukwu, J. (2024). A conceptual framework for context-aware data curation in fine-tuning pipelines. *International Journal of Engineering and Modern Technology, 10*(11), 197–228. https://doi.org/10.56201/ijemt.v10.no11.2024.pg197.228

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press. https://doi.org/10.4159/harvard.9780674736061

Perrow, C. (1984). *Normal accidents: Living with high-risk technologies*. Basic Books.

Raji, I. D., Smart, A., White, R. N., Mitchell, M., Gebru, T., Hutchinson, B., Smith-Loud, J., Theron, D., & Barnes, P. (2020). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. In *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* (pp. 33–44). ACM. https://doi.org/10.1145/3351095.3372873

Selbst, A. D. (2021). An institutional view of algorithmic impact assessments. *Harvard Journal of Law & Technology, 35*(1), 117–191.

Shahzadi, G., Jia, F., Chen, L., & John, A. (2024). AI adoption in supply chain management: A systematic literature review. *Journal of Manufacturing Technology Management, 35*(6), 1125–1150. https://doi.org/10.1108/JMTM-09-2023-0431

Sheffi, Y., & Rice, J. B. (2005). A supply chain view of the resilient enterprise. *MIT Sloan Management Review, 47*(1), 41–48.

Sodhi, M. S., & Tang, C. S. (2012). *Managing supply chain risk*. Springer. https://doi.org/10.1007/978-1-4614-3238-8

Tachizawa, E. M., & Wong, C. Y. (2014). Towards a theory of multi-tier sustainable supply chains: A systematic literature review. *Supply Chain Management: An International Journal, 19*(5/6), 643–663. https://doi.org/10.1108/SCM-02-2014-0070

United Nations. (2011). *Guiding principles on business and human rights: Implementing the United Nations "protect, respect and remedy" framework*. United Nations Human Rights Office of the High Commissioner.

Villena, V. H., & Gioia, D. A. (2018). On the riskiness of lower-tier suppliers: Managing sustainability in supply networks. *Journal of Operations Management, 64*, 65–87. https://doi.org/10.1016/j.jom.2018.09.004

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law, 7*(2), 76–99. https://doi.org/10.1093/idpl/ipx005

Wagner, B. (2019). Liable, but not in control? Ensuring meaningful human agency in automated decision-making systems. *Policy & Internet, 11*(1), 104–122. https://doi.org/10.1002/poi3.198

Wedraogo, L., Essandoh, S., Sakyi, J. K., Ibrahim, A. K., Okafor, C. M., Babalola, A. S., & Adenuga, M. A. (2025). Analysis of vendor management practices and their effects on supply chain performance. *International Journal of Multidisciplinary Futuristic Development, 6*(1), 42–54. https://doi.org/10.54660/IJMFD.2025.6.1.42-54

Wieland, A., & Durach, C. F. (2021). Two perspectives on supply chain resilience. *Journal of Business Logistics, 42*(3), 315–322. https://doi.org/10.1111/jbl.12271

Wu, L., Zhang, Z., Huang, J., Su, I.-H., & Tian, S. (2025). Digital technologies and supply chain resilience: A resource-action-performance perspective. *Information Systems Frontiers, 27*, 2137–2158. https://doi.org/10.1007/s10796-025-10595-1

Zamani, E. D., Smyth, C., Gupta, S., & Dennehy, D. (2023). Artificial intelligence and big data analytics for supply chain resilience: A systematic literature review. *Annals of Operations Research, 327*(2), 605–632. https://doi.org/10.1007/s10479-022-04983-y