Socio-Technical Governance of Information Asymmetry in Platform-Based Service Supply Chains

Emily Carter[1], Daniel Morales[2], Rachel Morgan[3],*

[1] Department of Information Systems, University of North Texas, Denton, TX 76203, United States
[2] Department of Supply Chain Management, Wright State University, Dayton, OH 45435, United States
[3] Department of Sociology, University of Nevada, Reno, NV 89557, United States

* Email: *rachel.morgan@unr.edu (Corresponding Author)*

Abstract

Platform-based service supply chains increasingly depend on cloud infrastructure, software providers, analytics vendors, cybersecurity intermediaries, and multi-sided client channels. In such settings, information asymmetry is not limited to private demand or hidden cost. It emerges from distributed data ownership, algorithmic opacity, uneven cyber-risk knowledge, contractual incompleteness, and unequal visibility into capacity conditions across B2B and B2C markets. This paper develops a socio-technical governance framework for information asymmetry in platform-based service supply chains. The framework integrates organizational governance, data governance, algorithmic accountability, cybersecurity assurance, and risk-sharing mechanisms into a unified decision architecture. A calibrated scenario analysis compares five governance regimes: baseline transparency, asymmetric disclosure, unmanaged multi-risk exposure, technical-control mitigation, and integrated socio-technical governance. Results show that purely technical controls reduce cyber exposure but leave substantial residual risk in capacity shortage, partner opportunism, and client trust loss. In contrast, integrated socio-technical governance reduces the normalized capacity shortage probability from 0.34 to 0.16, cyber exposure from 0.41 to 0.19, and client trust loss from 0.37 to 0.17, while increasing profit retention from 0.86 to 0.97. The findings indicate that platforms should treat information asymmetry as a governance problem that spans technology, contracts, incentives, and human oversight rather than as a narrow optimization error. The study contributes a practical governance matrix, scenario-based analytics, and implementation metrics for platform managers seeking resilient and trustworthy digital service supply chains.

Keywords: Platform-based service supply chains; information asymmetry; socio-technical governance; data governance; algorithmic accountability; cybersecurity assurance; risk sharing; resilient supply chain

Article History
Received: April 24, 2025
Revised: June 12, 2025
Accepted: August 06, 2025
Available Online: September 30, 2025

Socio-Technical Governance of Information Asymmetry in Platform-Based Service Supply Chains

1. Introduction

Digital service platforms have become essential intermediaries in contemporary supply chains. Enterprise resource planning systems, customer relationship management suites, payment gateways, cloud hosting services, cybersecurity monitoring tools, digital logistics platforms, and software-as-a-service applications increasingly operate through layered service ecosystems rather than through vertically integrated firms. These ecosystems connect infrastructure providers, platform operators, software vendors, analytics firms, channel partners, business clients, and individual users. Their economic value depends on availability, scalability, data reliability, pricing discipline, and trust. Yet these same properties also create persistent information asymmetry. A platform operator may understand demand better than an infrastructure provider, while the infrastructure provider may know more about cloud capacity, system congestion, energy costs, or service reliability. A cybersecurity vendor may observe vulnerabilities that clients do not see, while clients may possess private knowledge about transaction sensitivity, compliance exposure, or downstream reputational loss. This point is consistent with prior work on market opacity (Akerlof,1970). Algorithmic accountability research frames explainability as a governance requirement (Diakopoulos,2016).

The uploaded source manuscript motivating this study examines a dual-channel digital service supply chain in which a service provider sells to both B2B and B2C markets while relying on an infrastructure provider for the capacity needed to deliver the service. Its analytical emphasis is on stochastic demand, information asymmetry, demand risk, general supply chain risk, cybersecurity risk, and Stackelberg interaction between infrastructure and service providers. The present article develops a different but directly related research direction. Instead of deriving another profit-maximization model, it asks how socio-technical governance mechanisms should be designed when information asymmetry is embedded in the technological, contractual, and relational architecture of platform-based service supply chains. The same logic is supported by recent digital transformation research (Zhang and Lu,2025). Transparency research cautions that seeing data does not always mean understanding decisions (Ananny and Crawford,2018).

Information asymmetry has long been understood as a source of market inefficiency, adverse selection, and opportunistic behavior. In digital service ecosystems, however, asymmetry is more complex than one actor hiding a single cost or quality parameter. Data may be fragmented across application programming interfaces, telemetry systems, customer relationship databases, security logs, billing platforms, and service-level reports. Algorithmic pricing systems may produce decisions that are difficult to explain even to the managers responsible for them. Cybersecurity risks may remain invisible until a breach occurs. Capacity shortages may emerge gradually from forecast drift, cloud resource throttling, or service dependencies that were not represented in the original contract. The platform is therefore a socio-technical system: its risk performance depends on the interaction of data, technology, organizations, rules, incentives, and human judgment. Platform economics also explains this coordination problem (Parker and Van Alstyne,2005). Research on algorithmic opacity supports the concern about hidden model logic (Burrell,2016).

This socio-technical perspective is important because technical transparency alone does not eliminate strategic opacity. Dashboards may show current capacity utilization while hiding how costs are allocated. Blockchain systems may verify transaction records while failing to explain algorithmic prioritization. Artificial intelligence systems may improve demand prediction while generating new opacity through model complexity. Conversely, contracts may require disclosure but remain ineffective if the data infrastructure does not produce auditable evidence. Governance therefore requires alignment among information systems, platform incentives, contractual rights, cybersecurity assurance, and the social legitimacy of decision processes. Cyber supply chain studies reinforce the need for integrated assurance (Creazza et al.,2022). Ethics research on algorithms maps the

broader accountability debate (Mittelstadt et al.,2016).

The purpose of this study is to develop a governance-oriented analytical framework for information asymmetry in platform-based service supply chains. The article focuses on three research questions. First, what forms of information asymmetry matter most in digitally mediated service supply chains? Second, how do different governance mechanisms influence capacity shortage, cyber exposure, pricing distortion, and trust loss? Third, how should platform managers combine technical controls, contractual mechanisms, and human oversight to reduce residual risk across B2B and B2C channels? These questions extend the supply chain risk literature by shifting attention from isolated risk models to the governance systems that shape how risk information is generated, shared, interpreted, and acted upon. Platform governance research provides a useful design foundation (Gawer,2014). AI ethics studies show that principles require operational governance mechanisms (Jobin et al.,2019).

The study makes four contributions. First, it conceptualizes information asymmetry as a socio-technical condition that includes data asymmetry, algorithmic asymmetry, cyber-risk asymmetry, capacity asymmetry, and accountability asymmetry. Second, it develops a governance matrix linking each form of asymmetry to measurable operational proxies and decision rights. Third, it uses scenario analytics to compare the effects of baseline transparency, asymmetric disclosure, unmanaged risk exposure, technical controls, and integrated governance. Fourth, it provides managerial implementation guidance for designing risk-sharing agreements, audit routines, algorithmic oversight, and channel-specific assurance mechanisms. These contributions are especially relevant for platform businesses whose service reliability depends on external infrastructure and whose revenue is split across enterprise and consumer channels. Financial technology studies show that digital intermediation changes risk allocation (Kou and Lu,2025). Ethical AI research links accountability with human-centered institutional design (Floridi et al.,2018).

Figure 1 presents the conceptual landscape that guides the article. The figure intentionally avoids arrow-based causal simplification. It portrays the platform service supply chain as a set of layered governance zones in which infrastructure, platform operations, software service delivery, client relationships, and cybersecurity assurance coexist within a common governance boundary. The dashed and dotted regions highlight information asymmetry and cyber exposure as overlapping rather than separate problems. The implication is straightforward: governance design should not treat data sharing, cyber controls, and risk contracts as independent modules. Their combined effect determines whether the platform achieves resilient and trusted service delivery.

ISSN-3067-7505 https://doi.org/10.63646/jtis.2025.030303

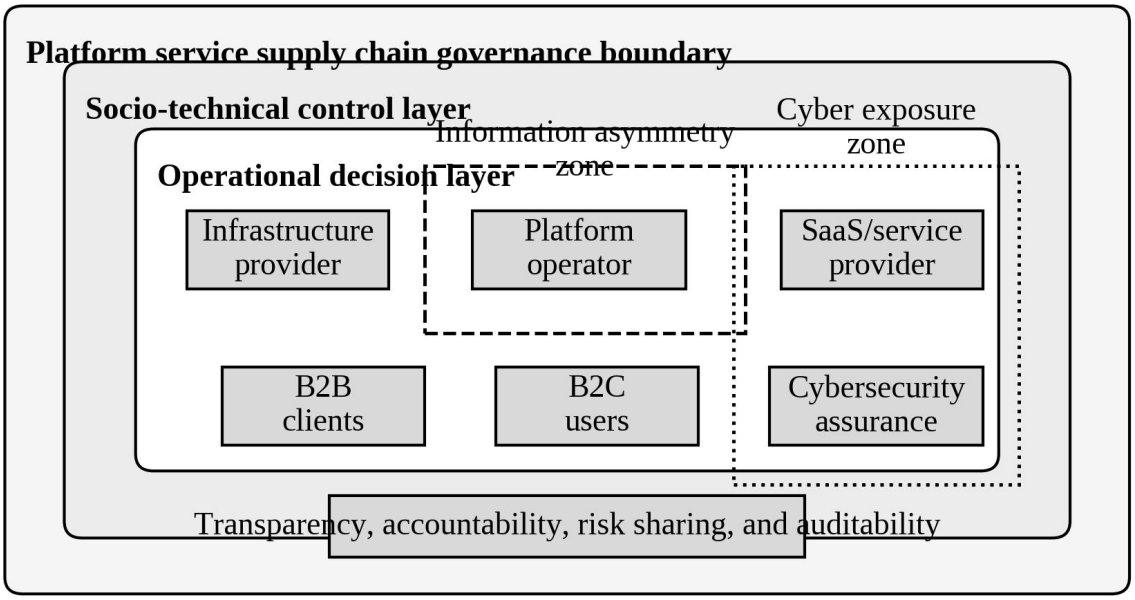

Figure 1. Socio-technical governance landscape for platform-based service supply chains.

2. Literature Review and Theoretical Background

Research on supply chain risk management has emphasized disruption preparedness, redundancy, flexibility, collaboration, and continuity planning. Traditional risk models often focus on physical flows, inventory, sourcing, and transportation. Digital service supply chains add a different set of dependencies. Service capacity may be elastic but not unlimited. Operational failures may originate from cloud configurations, software bugs, API outages, data quality degradation, or cybersecurity incidents. The result is a supply chain whose material flow is less visible than its information flow, but whose consequences are equally operational. A failure in an authentication service, a payment gateway, or a cloud resource allocation policy may interrupt service delivery as directly as a transportation delay interrupts product delivery. This view aligns with research on platform evolution and governance (Tiwana et al.,2010). Explainable AI research supports the movement from black-box systems toward glass-box systems (Rai,2020).

The resilience literature provides useful foundations for this discussion. Classic resilience scholarship argues that resilience requires visibility, velocity, flexibility, collaboration, preparation, and recovery capability. These ideas translate well into digital services, but they require reinterpretation. Visibility refers not only to inventory or shipments but also to real-time telemetry, service availability, error rates, capacity utilization, incident logs, and model performance. Flexibility refers not only to alternate suppliers but also to multi-cloud deployment, modular service architecture, failover routing, and contractually defined capacity buffers. Collaboration requires data-sharing routines, escalation rules, and mutual assurance rather than merely long-term supplier relationships. Digital supply chain twin research similarly emphasizes disruption-aware coordination (Ivanov and Dolgui,2021). Local explanation methods provide one practical tool for contestable model decisions (Ribeiro et al.,2016).

Information asymmetry remains a foundational explanation for inefficiency in supply chains and markets. Hidden quality can produce adverse selection when one party cannot observe the information held by another. Agency theory explains how actors with private information pursue their own interests under incomplete monitoring. In supply chains, asymmetry appears in private demand forecasts, hidden production costs, undisclosed capacity constraints, and quality uncertainty. Revenue-sharing and coordination contracts attempt to address such inefficiencies by aligning incentives across decentralized actors. However, platform-based service

supply chains differ from classic manufacturer-retailer days because they include digital traces, automated decision systems, cloud dependencies, and cybersecurity exposures that create new forms of opacity. Agency theory further clarifies the incentive problem (Eisenhardt,1989). Model interpretation research supports the use of feature-level explanation in audits (Lundberg and Lee,2017).

Platform studies explain why this problem is not merely operational. Multi-sided platforms coordinate interdependent participants whose decisions influence each other through network effects, pricing rules, data access, and governance boundaries. Platform leaders design access rules, technical interfaces, data standards, and dispute resolution procedures. In digital ecosystems, governance is partly architectural: the platform determines what actors observe, what actions they may take, what data are shared, and how accountability is assigned. A service supply chain platform therefore combines supply chain governance with ecosystem governance. Information asymmetry becomes a design outcome of platform architecture rather than an accidental imperfection. Industry 4.0 scholarship shows that digital connectivity reshapes operational governance (Lu,2025). Interpretability scholarship also calls for rigorous evaluation of explanation methods (Doshi-Velez and Kim,2017).

Digital innovation research reinforces this claim. Digital innovation can be understood as layered, recombinant, and generative, often emerging through distributed agency across heterogeneous actors. A platform-based service supply chain reflects the same logic: cloud infrastructure, application software, cybersecurity assurance, analytics, billing, and user interfaces are recombined into service offerings. Because different actors control different layers, no single actor has complete knowledge of the whole system. The governance problem is therefore not to eliminate all private information, which is unrealistic, but to design accountable information flows that reduce harmful asymmetry while respecting legitimate privacy, security, and commercial boundaries. Open-platform strategy research also highlights the role of access rules (Boudreau,2010). Algorithmic auditing research supports the need for end-to-end accountability processes (Raji et al.,2020).

Cybersecurity research further complicates the issue. Supply chain cyber risk is amplified by interconnected systems, third-party software, external APIs, shared identity infrastructure, and remote service access. Cybersecurity posture is often difficult to observe directly, creating a form of hidden action and hidden quality. A platform may claim that vendors meet security standards, but clients may not verify patch management, incident response capability, access control practices, or vulnerability disclosure. This makes cybersecurity assurance a core governance mechanism. Technical controls such as encryption, authentication, logging, and anomaly detection matter, but so do audit rights, disclosure duties, liability allocation, and escalation protocols. Empirical studies of analytics capability support this resilience interpretation (Dubey et al.,2021). Socio-technical fairness research warns against treating fairness as a purely technical abstraction (Selbst et al.,2019).

Algorithmic accountability literature provides another important foundation. Platforms increasingly use machine learning for demand forecasting, dynamic pricing, capacity allocation, fraud detection, and security monitoring. These systems improve responsiveness, but they also introduce model opacity and accountability gaps. Explainable artificial intelligence and model documentation provide tools for making decision systems more interpretable. Yet explanation alone is insufficient. A socio-technical governance approach requires defining who reviews models, when overrides are allowed, how errors are logged, how downstream stakeholders contest decisions, and how audit findings influence contracts and platform rules. Two-sided market theory explains why pricing and capacity decisions cannot be separated (Rochet and Tirole,2003). Data protection scholarship clarifies the limits of explanation rights (Wachter et al.,2017).

In summary, the literature suggests that information asymmetry in platform-based service supply chains is multidimensional. It includes private demand knowledge, hidden capacity conditions, cyber-risk opacity, data-quality uncertainty, model opacity, and weak accountability. Existing supply chain models provide rigorous tools for analyzing pricing and capacity decisions, while platform and algorithmic governance literatures explain how rules and architectures shape participant behavior. The gap addressed here lies at their intersection: the need for a

practical socio-technical governance framework that connects measurable service supply chain risks to information rights, technical controls, contract design, and organizational oversight. Blockchain-based auditing research illustrates how verification infrastructures reduce hidden actions (Wu et al.,2025). Disparate-impact research emphasizes the social consequences of data-driven decisions (Barocas and Selbst,2016).

3. Research Framework

The unit of analysis in this study is a platform-based service supply chain that delivers digital services through B2B and B2C channels. The focal platform procures infrastructure capacity from a cloud or infrastructure provider, combines this capacity with software and analytics capabilities, and offers differentiated service packages to enterprise and consumer markets. Enterprise customers typically demand contractual service levels, security certifications, integration support, and predictable capacity. Consumer users emphasize price, availability, usability, privacy, and trust. The same platform therefore faces different expectations, elasticities, and risk consequences across channels. Studies on platforms and infrastructures support this architectural view (Constantinides et al.,2018). Human-computer interaction research shows that transparency can shape trust in algorithmic interfaces (Kizilcec,2016).

The framework treats governance as a set of mechanisms that shape how information moves through the service supply chain. These mechanisms include technical systems, such as telemetry pipelines, shared dashboards, model monitoring, and security logging; contractual systems, such as service-level agreements, audit clauses, data-sharing obligations, and liability terms; organizational systems, such as joint risk committees, incident escalation routines, and human review of algorithmic decisions; and normative systems, such as fairness commitments, trust expectations, and platform responsibility. Each mechanism reduces one type of asymmetry while potentially creating another. For example, detailed security disclosure reduces client uncertainty but may expose sensitive vulnerability information if access is not governed. Industrial cyber-physical security research confirms the breadth of cyber exposure (Kayan et al.,2022). Research on invisible algorithms explains why users often infer rules from limited evidence (Eslami et al.,2015).

The framework distinguishes five asymmetric types. Data asymmetry occurs when actors observe different demands, capacity, quality, or incident information. Algorithmic asymmetry occurs when automated pricing, capacity allocation, or risk scoring systems are understood by one party but not by affected stakeholders. Cyber-risk asymmetry occurs when vulnerabilities, incidents, or control weaknesses are privately known. Contractual asymmetry occurs when service obligations, penalties, or exceptions are poorly understood or unevenly enforceable. Accountability asymmetry occurs when actors experience consequences without having meaningful access to evidence, explanation, or appeal. These asymmetries often interact. A capacity shortage may be a technical resource problem, but its governance failure may involve delayed disclosure, opaque allocation logic, and unclear compensation terms. Ecosystem innovation research reinforces the need for boundary governance (Gawer and Cusumano,2014). Algorithmic management research shows that automated decisions affect emotions and fairness perceptions (Lee,2018).

The first operational outcome is capacity shortage probability. In digital services, capacity shortage appears as latency, throttling, failed requests, degraded functionality, or inability to meet enterprise service levels. Unlike product shortages, capacity shortages may be temporary and hidden inside technical logs. The platform may know the shortage earlier than clients, while the infrastructure provider may know root causes earlier than the platform. Governance therefore requires predictive signals, transparent escalation thresholds, and contractual clarity about which actor is responsible for which class of shortage. Blockchain-IoT security research highlights the need for technical trust mechanisms (Xu et al.,2021). Society-in-the-loop research provides a useful model for institutionalizing accountability (Rahwan,2018).

The second operational outcome is cyber exposure. Cyber exposure refers to the likelihood and severity of harm arising from vulnerabilities, unauthorized access, credential misuse, software dependencies, data leakage, or

service disruption. It is not reducible to the presence or absence of security tools. It depends on how security telemetry is shared, how incidents are classified, how quickly vendors disclose threats, how clients are informed, and whether risk information is converted into business decisions. A platform with strong technical controls but weak incident governance may still create high exposure. Technology ecosystem governance research supports this multi-actor framing (Wareham et al.,2014). Workplace algorithm research explains why control becomes contested when decision systems are automated (Kellogg et al.,2020).

The third outcome is client trust loss. Trust loss reflects the reputational and relational effects of uncertainty, poor disclosure, unexplained pricing changes, opaque prioritization, and cybersecurity events. Trust is especially important on B2B channels, where enterprise clients depend on service continuity and compliance. It is also important for B2C channels, where users may exit quickly after perceived privacy or reliability failures. Prior research on online trust suggests that perceived integrity, competence, and predictability shape digital exchange behavior. In platform service supply chains, governance practices directly influence these perceptions. Sustainable supply chain research shows how distributed records can strengthen traceability (Saberi et al.,2019). Algorithmic management studies connect automated allocation with job design and work experience (Jarrahi et al.,2021).

The fourth outcome is profiting retention. Profit retention measures the share of potential profit preserved after accounting for capacity loss, price distortion, cyber exposure, compensation costs, and trust-related churn. Unlike conventional profit analysis, profit retention highlights the governance value of preventing avoidable losses. It is not a precise accounting metric in this study; rather, it functions as an integrative analytical indicator linking service reliability, cyber assurance, client trust, and maturity. Table I summarizes the major constructs and operational proxies used in the framework. Ecosystem strategy research explains why governance must define actor roles (Adner,2017). Algorithm ethics research clarifies how responsibility extends from design to use (Parent-Rocheleau and Parker,2022).

Table I. Governance Constructs and Measurement Proxies

Governance construct	Main asymmetry addressed	Operational proxy	Illustrative decision right
Data transparency	Demand and capacity asymmetry	Forecast error, missing telemetry, update latency	Right to request capacity evidence
Algorithmic accountability	Pricing and allocation opacity	Explanation coverage, override rate, model drift	Right to human review of high-impact decisions
Cybersecurity assurance	Hidden vulnerability and incident knowledge	Patch age, incident severity, audit exceptions	Right to receive tiered incident disclosure
Risk-sharing contract	Opportunistic risk transfer	Penalty balance, early-warning compliance	Right to renegotiate after documented risk change
Client trust governance	Accountability asymmetry	Churn, complaint rate, service-credit disputes	Right to explanation and documented remediation

4. Methodology and Scenario Design

This article uses calibrated scenario analytics rather than empirical estimation from proprietary platform data. The purpose is to compare governance regimes under consistent assumptions and to reveal the mechanisms through which information asymmetry affects service supply chain performance. The scenario design follows a single-period planning logic common in capacity and pricing models, but the interpretation is governance-oriented. Each scenario represents a different configuration of information rights, technical visibility, contractual accountability, and human oversight. Information systems scholarship on blockchain supports this transparency mechanism (Lu,2022). Algorithm aversion research shows that acceptance depends on perceived reliability and fairness (Martin,2019).

The first scenario, baseline transparency, assumes that platform actors share reliable demand, capacity, and incident information and that contractual obligations are clear. This scenario serves as a normative benchmark rather than as a common operating reality. The second scenario, asymmetric disclosure, introduces private information. The platform has better knowledge of demand and customer urgency, while the infrastructure provider has better knowledge of capacity constraints and cost volatility. The cybersecurity vendor has partial

knowledge of vulnerabilities, and clients observe only service outcomes. The third scenario, unmanaged multi-risk exposure, adds demand volatility, supply disruption, cyber exposure, and weak escalation routines. It represents the situation in which information asymmetry is compounded by insufficient governance. The ecosystem literature also emphasizes complementarity among actors (Jacobides et al.,2018). Technology ethics research also reinforces accountability across the platform lifecycle (Mahmud et al.,2022).

The fourth scenario, technical-control mitigation, introduces dashboards, monitoring, anomaly detection, automated alerts, and security hardening. These controls reduce some cyber and capacity risks, but they do not fully address opportunistic disclosure, contract ambiguity, or contested decision rights. The fifth scenario, integrated socio-technical governance, combines technical controls with audit clauses, risk-sharing contracts, joint incident review, algorithmic accountability, channel-specific assurance, and client-facing explanation protocols. This scenario represents a more mature governance design that treats transparency, resilience, and trust as linked outcomes. Digital supply chain defense research shows that governance capability accumulates over time (Boyson et al.,2022).

The scenario parameters were selected to reflect a medium-sized digital service platform with two major customer channels. The B2B channel accounts for fewer customers but has higher revenue per account, stricter service levels, and higher cyber sensitivity. The B2C channel accounts for larger transaction volume, higher churn sensitivity, and greater privacy visibility. The platform relies on an external infrastructure provider for scalable capacity and uses third-party tools for security monitoring and analytics. Table II provides the operational assumptions used in the scenario analysis. Digital innovation theory supports this layered understanding of platform services (Yoo et al.,2010).

The analysis uses normalized indices between 0 and 1 for three primary risk outcomes: capacity shortage probability, cyber exposure, and client trust loss. Profit retention is represented as the retained share of potential profit after risk-related loss. These values should not be interpreted as universal empirical estimates. They are decision-analytic outputs designed to compare governance regimes. This approach is appropriate for early-stage governance design, where managers often lack complete historical data but still need structured reasoning about alternative governance investments. Data-driven refinements could later replace the calibrated values with platform telemetry, security logs, customer churn data, and incident records. Blockchain research in enterprise systems further connects governance with information integrity (Zheng and Lu,2022).

The scenario logic also incorporates a maturity scale from 1 to 5. Level 1 represents fragmented governance: local data ownership, informal disclosure, weak auditability, and reactive incident response. Level 2 introduces basic documentation and contract templates. Level 3 adds shared dashboards, security baselines, and periodic review. Level 4 adds predictive risk monitoring, role-based information access, and joint risk governance. Level 5 integrates technical, contractual, and social accountability, including model explainability, audit logs, risk-sharing incentives, channel-specific assurance, and client notification standards. This maturity scale is used in Figure 4 to evaluate how residual risk changes as governance capabilities deepen. Digital innovation management research reinforces the importance of recombination and governance (Nambisan et al.,2017).

The methodological contribution of this design is not mathematical complexity. Its value lies in making governance comparable across socio-technical dimensions. Managers often invest in cybersecurity tools, data platforms, or contract revisions separately. The scenario method shows why separate investment creates uneven risk reduction. Technical control may reduce cyber exposure but leaves trust loss high if clients receive no explanation. A contract may allocate liability but fail to prevent shortage if capacity telemetry is late. A dashboard may increase visibility but create information overload if decision rights are unclear. Integrated governance performs better because it connects evidence, authority, incentives, and accountability. IoT-enabled supply chain research explains why cyber-physical visibility matters (Ben-Daya et al.,2019).

Table II. Scenario Design and Parameterization

Scenario	Information regime	Technical visibility	Governance maturity	Expected managerial

				condition
S1 Baseline transparency	Reliable shared disclosure	Common dashboard and logs	Level 4	Collaborative platform-infrastructure relationship
S2 Asymmetric disclosure	Private demand and capacity knowledge	Partial dashboards	Level 2	Strategic withholding and incomplete contracts
S3 Unmanaged multi-risk exposure	Fragmented and delayed disclosure	Reactive monitoring	Level 1	Demand volatility, cyber risk, and weak escalation
S4 Technical-control mitigation	Telemetry improves but rights remain unclear	Automated alerts and anomaly detection	Level 3	Technology investment without full accountability
S5 Integrated socio-technical governance	Accountable disclosure with audit rights	Shared evidence, review, and assurance	Level 5	Coordinated governance across data, contracts, and people

5. Analysis and Findings

The first finding is that information asymmetry creates risk pressure across multiple pathways rather than through a single channel. Figure 2 shows governance pressure scores for five risk pathways across six governance dimensions. Capacity shortage is especially sensitive to data quality, risk sharing, and transparency. Pricing distortion is sensitive to contract design and transparency. Cyber exposure is most sensitive to assurance mechanisms, human oversight, and data quality. Partner opportunism is most sensitive to transparency, contracts, and risk-sharing structure. Client trust loss is most sensitive to human oversight, data quality, and assurance. The heatmap demonstrates that no single governance dimension resolves all risks. Digital transformation research similarly treats governance as organizational change (Verhoef et al.,2021).

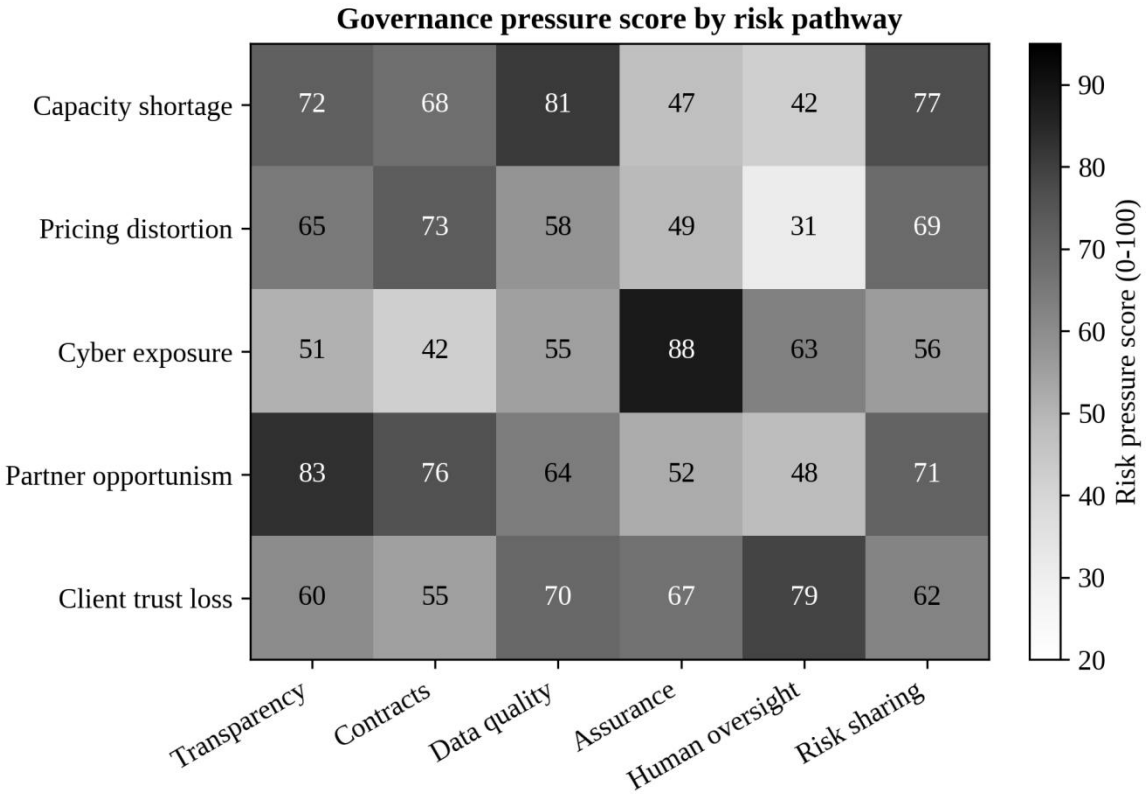

Figure 2. Governance pressure score by risk pathway and governance dimension.

The heatmap highlights why governance should be treated as a portfolio. Darker cells show that high pressure may arise from data quality, risk sharing, contracts, or assurance depending on the risk pathway.

This finding has practical significance. A platform may invest heavily in security assurance and still leave capacity shortage unmanaged if demand and capacity information remain misaligned. Another platform may

improve contracts while leaving algorithmic prioritization unexplained. The governance problem is therefore one of portfolio design. The platform needs a bundle of mechanisms that cover different asymmetric pathways. This resembles the logic of supply chain resilience, where redundancy, flexibility, visibility, and collaboration complement rather than substitute for one another. Cloud pricing research supports the relevance of capacity and quality-of-service allocation (Lu et al.,2020).

The second finding is that unmanaged multi-risk exposure creates a sharp increase in normalized risk outcomes. Table III reports scenario-level results. In the baseline transparency scenario, capacity shortage probability is 0.12, cyber exposure is 0.18, client trust loss is 0.10, and profit retention is 0.96. Under asymmetric disclosure, shortage probability rises to 0.22, cyber exposure to 0.28, trust loss to 0.25, and profit retention falls to 0.91. Under unmanaged multi-risk exposure, shortage probability reaches 0.34, cyber exposure 0.41, trust loss 0.37, and profit retention falls to 0.86. These changes illustrate how information asymmetry amplifies the consequences of demand volatility, infrastructure uncertainty, and cyber vulnerability. Strategic information systems research clarifies why transformation is more than technology adoption (Vial,2019).

Table III. Scenario Results for Governance Alternatives

Scenario	Capacity shortage probability	Cyber exposure index	Client trust loss index	Profit retention ratio
S1 Baseline transparency	0.12	0.18	0.10	0.96
S2 Asymmetric disclosure	0.22	0.28	0.25	0.91
S3 Unmanaged multi-risk exposure	0.34	0.41	0.37	0.86
S4 Technical-control mitigation	0.25	0.24	0.30	0.91
S5 Integrated socio-technical governance	0.16	0.19	0.17	0.97

Table III translates the qualitative governance regimes into comparable normalized indicators. It shows that integrated socio-technical governance recovers more risk value than technical mitigation alone.

The third finding is that technical controls are necessary but insufficient. In the technical-control mitigation scenario, cyber exposure falls from 0.41 to 0.24 and capacity shortage probability falls from 0.34 to 0.25. However, client trust loss remains at 0.30, and profit retention improves only to 0.91. The reason is that technical controls reduce incident likelihood and improve detection but do not automatically produce legitimate governance. Clients and partners still need to know how decisions are made, how service degradation is allocated across channels, how data are used, and how accountability is enforced. This aligns with algorithmic accountability research showing that prediction accuracy alone does not establish trust or governance legitimacy. Machine-learning risk prediction research supports the use of interpretable analytics (Baryannis et al.,2019).

The fourth finding is that integrated socio-technical governance produces the strongest improvement across all metrics. The integrated scenario reduces capacity shortage probability to 0.16, cyber exposure to 0.19, and client trust loss to 0.17, while increasing profit retention to 0.97. The improvement is not due to one mechanism. It results from aligning capacity telemetry, contractually defined risk sharing, cybersecurity assurance, client notification rules, algorithmic explanation, and human review. The result resembles a coordination effect: each mechanism improves the operating conditions for the others. Shared data improve forecasting; audit rights make disclosure credible; risk sharing reduces opportunism; human oversight improves the legitimacy of algorithmic allocation; and client communication reduces trust loss. Innovation management studies also connect transformation with organizational redesign (Appio et al.,2021).

Figure 3 compares the five scenarios visually. The pattern is instructive. Asymmetry increases all three risk scores, unmanaged exposure increases them further, technical controls reduce cyber exposure more than trust loss, and integrated governance provides balanced reduction. The difference between technical controls and integrated governance is especially important. In many platform firms, cyber-risk management is treated as a technology domain, while client trust and contract design are treated as legal or commercial domains. The scenario results suggest that this separation is harmful. Cybersecurity risk has social and contractual consequences, and information asymmetry has technical causes. Governance should therefore be designed at their intersection.

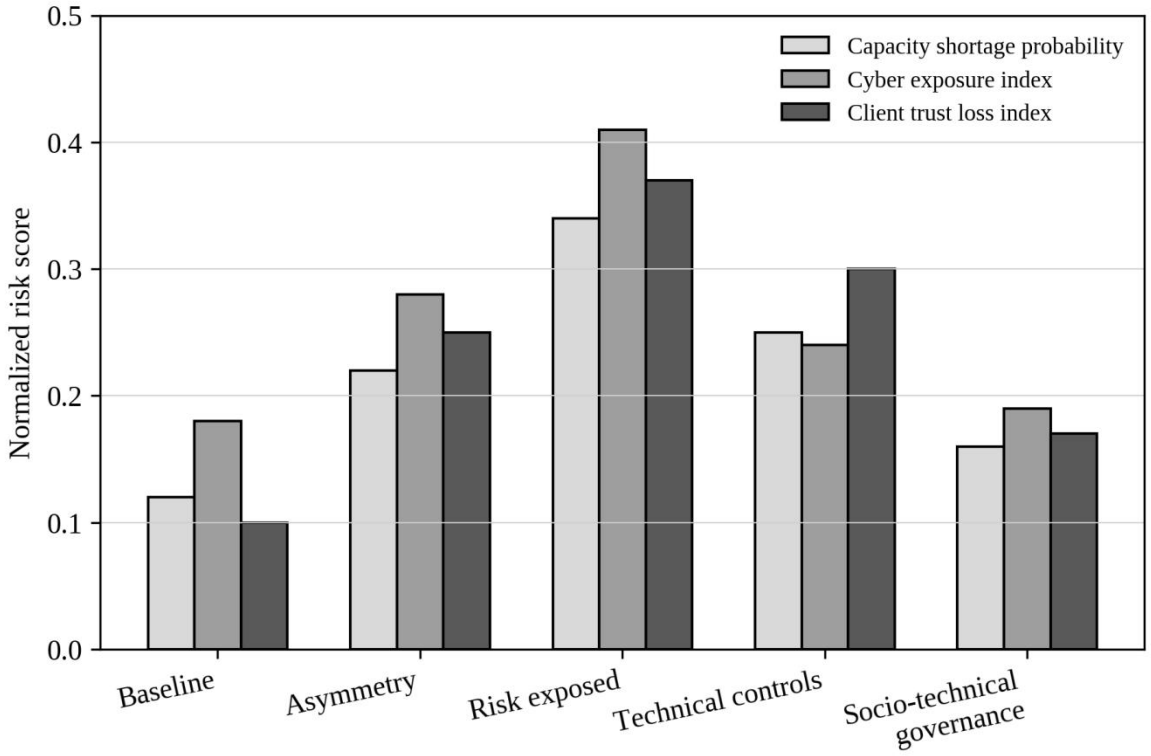

Figure 3. Scenario comparison of capacity shortage probability, cyber exposure, and client trust loss.

Figure 3 confirms that technical controls reduce cyber exposure more strongly than trust loss, whereas integrated governance reduces all three risk indicators in a more balanced way.

The fifth finding concerns maturity. Figure 4 shows that residual shortage and cyber exposure decline steadily as maturity increases, while profit retention rises. The largest marginal improvement occurs between maturity Levels 2 and 4, where firms move from documentation and basic monitoring to shared dashboards, predictive risk monitoring, and joint governance. Level 5 still improves performance, but the marginal gain is smaller because the most severe gaps have already been addressed. This pattern suggests a staged investment strategy. Firms with fragmented governance should first build shared evidence and basic accountability. More mature firms should invest in explanation systems, channel-specific assurance, and continuous governance review.

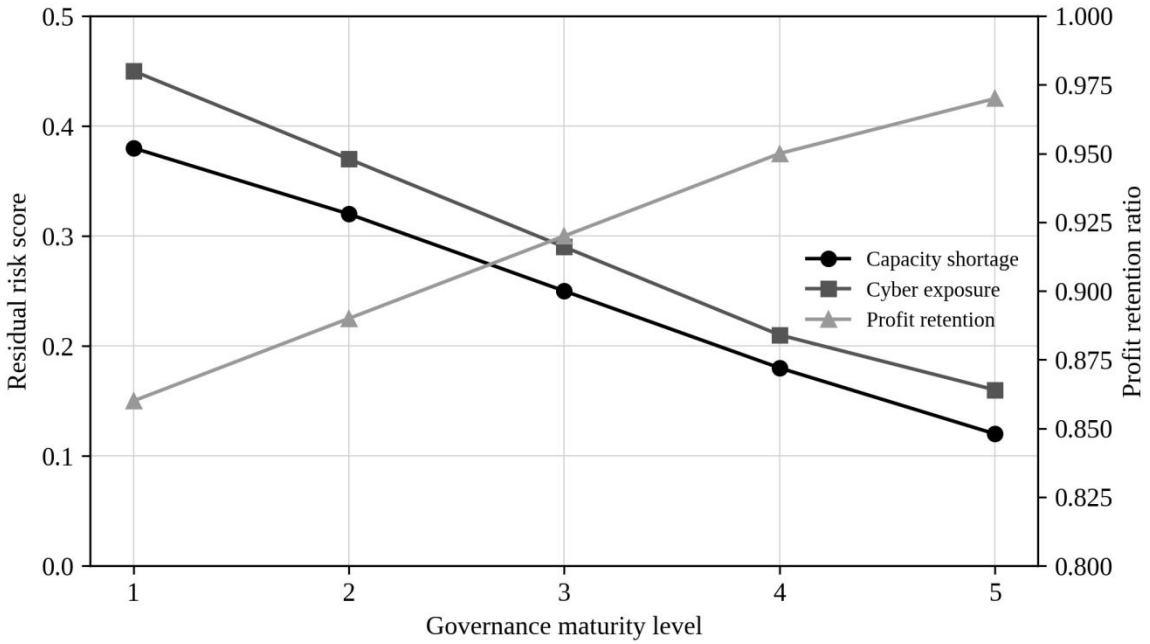

Figure 4. Governance maturity, residual risk, and profit retention.

Figure 4 indicates that the most important maturity transition occurs when firms move from basic documentation toward predictive monitoring, shared evidence, and joint governance review.

The sixth finding concerns channel heterogeneity. Figure 5 decomposes channel-level risk across B2B direct contracts, B2B reseller partners, B2C subscription users, and B2C freemium users. B2B channels carry higher information and capacity risk because enterprise service-level commitments create costly shortage consequences and because reseller partners may introduce additional disclosure layers. B2C channels carry higher cyber and compliance-related trust risk because privacy concerns, data-use expectations, and high-volume user interactions amplify reputational effects. A uniform governance policy therefore wastes resources. Enterprise contracts require stronger capacity assurance and transparent prioritization rules. Consumer-facing services require privacy-by-design, visible incident communication, and explainable automated decisions.

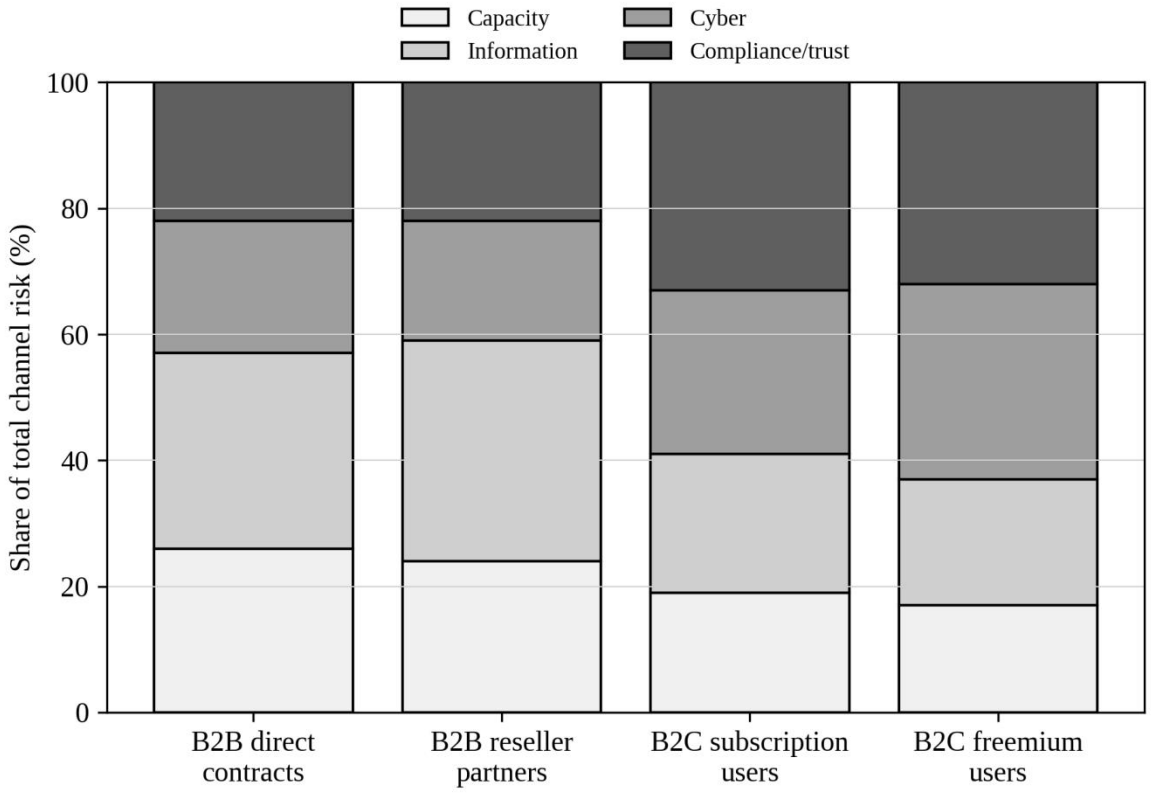

Figure 5. Channel-level risk composition across B2B and B2C service segments.

Figure 5 supports differentiated governance by channel. Enterprise channels require stronger capacity and information assurance, while consumer channels require stronger privacy, compliance, and trust governance.

The seventh finding is that governance creates value partly by reducing ambiguity before crises occur. When platform actors know what information must be shared, when alerts escalate, how compensation is calculated, and which human decision body reviews exceptional cases, they reduce delay during incidents. This is critical in digital services because operational windows are short. Capacity degradation or cyber exposure may escalate within minutes. Contracts drafted only for post-event liability do not reduce real-time harm. Governance must therefore combine pre-defined protocols with live telemetry and delegated authority. IoT cybersecurity research confirms that connected service systems expand risk surfaces (Lu and Xu,2019).

6. Discussion

The findings support a central proposition: information asymmetry in platform-based service supply chains should be governed as a socio-technical condition rather than treated as an isolated economic distortion. In the source risk-management tradition, asymmetry affects capacity and pricing decisions through private information and strategic interaction. This article extends that logic by showing that asymmetry also shapes the legitimacy, auditability, and resilience of digital service systems. The platform does not merely decide how much capacity to buy or what price to charge. It decides who sees information, who interprets anomalies, whose preferences are represented in algorithms, and who bears residual risk after a failure. Recent management research on digital transformation supports the need for implementation of roadmaps (Plekhanov et al.,2023).

This perspective changes the role of data governance. In many organizations, data governance is framed as metadata management, data quality, or privacy compliance. In platform service supply chains, it also becomes a coordination mechanism. Shared definitions of capacity, downtime, breach severity, incident priority, and customer impact are necessary for aligning service expectations. Without common definitions, each actor may

interpret the same event differently. A platform may classify a slowdown as minor degradation; an enterprise client may classify it as a contractual breach; an infrastructure provider may classify it as normal variance. Data governance reduces this interpretive asymmetry by establishing common operational language. Empirical blockchain adoption research illustrates why governance barriers cannot be ignored (Queiroz and Fosso Wamba,2019).

The analysis also clarifies the limits of transparency. Full transparency is neither feasible nor always desirable. Infrastructure providers may protect sensitive security details. Platform firms may protect proprietary demand models. Clients may protect transaction data. The governance task is therefore not total disclosure but accountable disclosure. Accountable disclosure means that relevant information is available to the right parties, at the right time, at the right level of detail, under auditable access rules. This is consistent with contextual approaches to digital governance, where the legitimacy of information flow depends on purpose, role, and expectation rather than on disclosure volume alone. Organizational studies of digital transformation emphasize strategy and change alignment (Hanelt et al.,2021).

Algorithmic governance is especially important because automated systems increasingly allocate scarce capacity, detect anomalies, set prices, and flag risk. Such systems may reduce human bias and improve speed, but they may also hide assumptions and create unfair outcomes. A B2B client whose workload is throttled during peak demand may ask whether the decision was based on contract tier, profitability, latency sensitivity, or an opaque machine-learning score. A B2C user facing a price change may question whether the change reflects demand, risk, or discriminatory segmentation. Explanation mechanisms, audit logs, and human review reduce these concerns by linking decisions to accountable rules. Big-data operations research supports the value of analytics in operational decision-making (Choi et al.,2018).

Cybersecurity assurance illustrates the value of integrated governance. A platform may implement strong technical controls, but if vendors delay vulnerability disclosure or if clients do not know the incident classification process, residual risk remains high. Conversely, contracts may require disclosure within a specific number of hours, but if logging systems lack reliable evidence, disclosure becomes incomplete. Integrated assurance combines technical monitoring, independent audit, disclosure protocols, insurance or liability terms, and post-incident learning. This combination is particularly important because cyber events frequently cross organizational boundaries and expose weaknesses in partner governance rather than only in technology. Digital platform ecosystem research clarifies how interdependent actors co-create value (Hein et al.,2020).

The findings also suggest that risk-sharing contracts should be designed around behavior, not only outcomes. Traditional service-level agreements penalize downtime or non-delivery after the fact. In digital service ecosystems, governance should also reward early disclosure, accurate forecasting, joint remediation, and preventive investment. A provider that reports emerging capacity constraints early should not be punished in the same way as a provider that hides the risk until service fails. Similarly, a platform that shares realistic demand forecasts should receive better capacity terms than one that strategically inflates forecasts. Behavioral incentives reduce opportunism by making transparency economically rational. Big-data capability research shows that analytics influences organizational performance (Wamba et al.,2017).

Finally, socio-technical governance provides a bridge between managerial efficiency and social legitimacy. Platform-based services influence enterprise operations, consumer privacy, labor processes, and public trust. Governance arrangements that appear efficient internally may create external distrust if decisions are unexplained or accountability is weak. Technology innovation and society perspective is therefore essential. Service supply chain governance is not only about maximizing platform profit; it is also about designing digital interdependence in ways that are reliable, contestable, secure, and fair. Supply chain integration research supports the operational value of shared information (Rai et al.,2006).

7. Managerial Implications

Platform managers should begin by mapping information asymmetry across the service supply chain. The mapping should identify which actor holds superior knowledge about demand, capacity, incidents, vulnerabilities, costs, client urgency, and algorithmic decision logic. This mapping should not remain a conceptual exercise. Each asymmetry should be linked to observable evidence, such as dashboard fields, logs, audit reports, contract clauses, exception approvals, or client notifications. Table IV presents a practical governance matrix connecting mechanisms to implementation indicators. Blockchain adoption research further clarifies why institutional barriers shape implementation (Kouhizadeh et al.,2021).

Table IV. Governance Mechanisms and Implementation Metrics

Mechanism	Implementation practice	Primary metric	Expected governance benefit
Shared telemetry	Real-time service and capacity dashboard with common definitions	Update latency; missing data rate	Reduces data asymmetry and forecast disputes
Audit-ready contracts	Clauses for data access, incident evidence, and early warning	Disclosure compliance rate	Reduces strategic withholding and post-event conflict
Algorithmic review	Model cards, explanation reports, and override logs	Explanation coverage; override closure time	Reduces algorithmic asymmetry and legitimacy loss
Cyber assurance	Independent audits, vendor security attestations, and tiered incident disclosure	Patch age; audit exception count	Reduces hidden vulnerability risk
Joint risk committee	Monthly scenario review and emergency escalation authority	Escalation time; action completion rate	Aligns technical evidence with organizational authority

Table IV turns the governance framework into implementable metrics. Each mechanism is linked to a concrete practice, a measurable indicator, and the benefit of governance expected from adoption.

The first managerial implication is that shared dashboards should be paired with decision rights. Visibility without authority produces frustration rather than governance. If enterprise clients see service degradation but lack escalation rights, transparency may increase dissatisfaction. If infrastructure providers see demand surges but lack contractual authority to request capacity adjustments, early warning may not lead to action. Each dashboard metric should therefore be associated with a responsible actor, a response time, an escalation path, and a documented consequence. Resilience research after COVID-19 supports a cross-industry view of service continuity (Belhadi et al.,2021).

The second implication is that platforms should use differentiated governance for B2B and B2C channels. B2B clients require stronger capacity assurance, clearer incident escalation, auditable service-level evidence, and negotiated risk-sharing. B2C users require privacy clarity, visible reliability indicators, straightforward communication, and fair automated decisions. The same technical infrastructure supports both channels, but the governance interface should reflect channel-specific risks. This is especially important when a platform prioritizes enterprise traffic during capacity shortages. Without transparent rules, prioritization may appear opportunistic or unfair. Blockchain sustainability research also links transparency with accountability outcomes (Park and Li,2021).

The third implication is that cybersecurity investment should be evaluated as a trust and governance investment, not only as a technical cost. The scenario results show that cyber exposure and trust loss move together but are not identical. Security tools reduce exposure, while disclosure and accountability reduce trust loss. Managers should therefore budget for incident communication, audit readiness, vendor assurance, access governance, and post-incident learning alongside technical tools. The return on cybersecurity governance includes avoided churn, reduced contract disputes, faster recovery, and stronger platform reputation. Disruption analytics research demonstrates why scenarios are useful for stress testing (Ivanov,2020).

The fourth implication is that contracts should specify information duties before specifying penalties. Penalty clauses matter, but they are reactive. Information duties define the conditions under which partners must share forecasts, capacity warnings, cyber incidents, model changes, and service degradation evidence. Contracts should be distinguished between routine data sharing, early-warning disclosure, emergency disclosure, and post-incident

evidence. They should also define confidentiality protections to ensure that legitimate commercial or security concerns do not prevent useful governance transparency. A broader blockchain review supports the need for classification and open-issue analysis (Casino et al.,2019).

The fifth implication is that algorithmic oversight should include both model performance and stakeholder impact. Platforms often monitor prediction accuracy or error rates, but governance requires additional metrics: explanation coverage, override frequency, escalation time, dispute resolution, channel fairness, and audit exceptions. These metrics connect technical model performance with social accountability. A model that predicts demand accurately but allocates scarce capacity in ways that violate service commitments remains a governance failure. Viable supply chain theory reinforces the joint role of agility, resilience, and sustainability (Ivanov,2022).

The sixth implication is that integrated governance should be implemented in stages. Firms at maturity Level 1 should start with operational definitions, incident taxonomies, and minimal shared evidence. Level 2 firms should formalize contracts and service-level metrics. Level 3 firms should implement shared dashboards, data-quality controls, and basic cyber assurance. Level 4 firms should add predictive monitoring, joint risk committees, and algorithmic review. Level 5 firms should institutionalize continuous audit, scenario rehearsal, channel-specific trust mechanisms, and independent governance review. This staged path prevents organizations from overinvesting in advanced tools before they have reliable data and accountability foundations. Cyber supply chain risk management research supports the strategic control perspective (Boyson,2014).

8. Policy and Societal Implications

Platform-based service supply chains increasingly support critical organizational processes. When they fail, the effects may spread across clients, workers, consumers, and public services. This gives information asymmetry a societal dimension. If platforms conceal capacity fragility, cyber exposure, or algorithmic prioritization rules, affected stakeholders may be unable to protect themselves. Policy debates about platform accountability should therefore extend beyond content moderation and consumer privacy to include service reliability, supply chain transparency, and digital infrastructure dependence. Classic resilience research emphasizes visibility and collaboration as core principles (Christopher and Peck,2004).

Regulators and industry bodies may encourage common disclosure standards for digital service supply chains. Such standards need not require public release of sensitive security details. Instead, they could define minimum categories of information that must be documented and auditable: service dependency maps, incident classification procedures, third-party assurance results, capacity shortage notification rules, and algorithmic decision review processes. Standardized disclosure reduces the cost of evaluating service providers and may limit adverse selection in digital service markets. Artificial intelligence research supports the role of algorithmic decision support.

Policy should also recognize the tension between transparency and security. Excessive disclosure of vulnerabilities may increase attack risk, while insufficient disclosure undermines trust and accountability. A tiered disclosure model is preferable. Internal operations teams receive detailed telemetry. Contracted clients receive service impact and assurance evidence. Public users receive clear explanations of major incidents and protections. Auditors receive controlled access to sensitive evidence. This layered approach balances security, accountability, and commercial confidentiality. Robust supply chain strategy research clarifies the importance of mitigation portfolios (Tang,2006).

Finally, social legitimacy depends on contestability. Stakeholders affected by capacity allocation, cyber incidents, or automated decisions should have meaningful channels for inquiry and redress. Contestability does not mean that every operational decision becomes negotiable. It means that affected parties are able to obtain explanations, challenge errors, and receive documented responses. As digital service platforms become infrastructure-like, contestability becomes part of responsible technology governance. Cyber-physical systems research confirms that security risks are architectural and organizational (Yaacoub et al.,2020).

9. Limitations and Future Research

This study has limitations. The scenario analysis is calibrated rather than estimated from proprietary platform data. The values are useful for comparing governance regimes, but they are not presented as universal empirical measurements. Future research should estimate the framework using transaction logs, service-level records, cloud capacity data, security incident data, and client churn observations. Such empirical work would allow researchers to test whether the relationships observed in the scenario analysis hold across industries, platform sizes, and governance structures. Supply chain risk management studies connect practices with performance outcomes (Wieland and Wallenburg,2012).

A second limitation is that the analysis uses normalized risk indices. These indices make comparison easier, but they abstract from detailed financial and operational mechanisms. Future work could combine the governance framework with stochastic optimization, agent-based modeling, or system dynamics. This would allow researchers to examine how information asymmetry evolves over time, how actors learn from incidents, and how risk-sharing contracts influence long-term investment in transparency and resilience. Recent IoT security surveys highlight the complexity of cyber-physical service environments.

A third limitation is that the paper focuses primarily on infrastructure provider, platform operator, service provider, and client relationships. Many platform service supply chains include additional actors, such as payment processors, identity providers, data brokers, cybersecurity insurers, regulators, and reseller networks. Future research should examine multi-actor governance networks in which accountability is distributed across several layers. This is especially important for cross-border digital services, where regulatory jurisdiction and data localization rules create additional asymmetry. Early supply chain risk research frames risk management as a forward-looking agenda (Jüttner et al.,2003).

A fourth limitation concerns algorithmic governance. The article identifies algorithmic asymmetry as a key mechanism, but it does not test specific explainability methods or model governance tools. Future research should evaluate how explanation interfaces, model cards, audit trails, and override procedures influence stakeholder trust, decision speed, and error correction. Such work would deepen the connection between explainable artificial intelligence and service supply chain governance. Cyber-physical system security research shows why layered protection is needed (Humayed et al.,2017).

Future studies should also investigate how platform governance interacts with sustainability. Digital service infrastructure consumes energy, requires data centers, and relies on hardware supply chains. Capacity governance therefore has environmental implications. Information asymmetry about energy use, cloud region selection, and carbon intensity may influence enterprise purchasing decisions and regulatory compliance. Integrating environmental data into service supply chain governance would extend this framework toward responsible digital infrastructure management. Industrial cybersecurity research highlights the special vulnerability of critical infrastructure.

10. Conclusion

This study developed a socio-technical governance framework for information asymmetry in platform-based service supply chains. It argued that information asymmetry in digital services is not limited to hidden demand or private costs. It also includes data asymmetry, algorithmic opacity, cyber-risk uncertainty, contractual ambiguity, and accountability gaps across infrastructure providers, platform operators, software providers, enterprise clients, and consumer users. These forms of asymmetry interact with demand volatility, capacity shortage, cybersecurity exposure, and trust loss.

The scenario analysis showed that unmanaged asymmetry and multi-risk exposure substantially increase capacity shortage probability, cyber exposure, and client trust loss. Technical controls reduce important risks, particularly cyber exposure, but they leave residual governance weaknesses when decision rights, contracts, human oversight, and client communication remain underdeveloped. Integrated socio-technical governance

produces the strongest overall performance because it connects evidence, authority, incentives, and accountability. It reduces risk more evenly across operational and trust-based outcomes and improves profit retention.

For platform managers, the central implication is clear. Governance should be designed as an integrated system rather than as a collection of isolated controls. Shared dashboards require decision rights. Cybersecurity tools require disclosure protocols. Contracts require data evidence. Algorithms require explanation and review. B2B and B2C channels require differentiated assurance. Mature platform governance links technical visibility with social legitimacy, making service supply chains more reliable, auditable, and trustworthy.

The broader contribution of the article is to place supply chain risk management within the technology innovation and society perspective. Platform-based service supply chains are not only operational systems. They are social and technical arrangements that shape how organizations and users experience digital dependence. Responsible governance of information asymmetry is therefore central to the future of digital service ecosystems.

Acknowledgement

The authors thank the anonymous reviewers and editorial team for their constructive suggestions. The authors also acknowledge the institutional research environments that supported this work.

Author Contributions

Table V. Author Contributions

Author	Contribution
Emily Carter	Conceptualization, writing - original draft, methodology, visualization
Daniel Morales	Scenario analysis, data curation, formal analysis, writing - review and editing
Rachel Morgan	Supervision, socio-technical governance framework, validation, project administration

Declarations

Conflicts of interest: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this manuscript.

Data availability: No proprietary dataset is redistributed in this manuscript. The scenario values and aggregated figures are available from the corresponding author upon reasonable request.

Funding: This research received no external funding.

Ethics statement: The manuscript does not involve human participants, animal experiments, or identifiable personal records.

About the Authors

Emily Carter is affiliated with the University of North Texas, United States. Her research focuses on digital service platforms, data governance, and information systems strategy.

Daniel Morales is affiliated with Wright State University, United States. His research interests include service supply chains, platform operations, and risk analytics.

Rachel Morgan is affiliated with the University of Nevada, Reno, United States. Her work examines socio-technical governance, technology accountability, and organizational trust in digital ecosystems.

Reference

Akerlof, G. A. (1970). The market for lemons: Quality uncertainty and the market mechanism. Quarterly Journal of Economics, 84(3), 488–500. DOI: 10.2307/1879431

Zhang, H., & Lu, Y. (2025). Web 3.0: Applications, opportunities and challenges in the next internet generation. Systems Research and

Behavioral Science, 42(4), 996–1015. DOI: 10.1002/sres.3151

Parker, G. G., & Van Alstyne, M. W. (2005). Two-sided network effects: A theory of information product design. Management Science, 51(10), 1494–1504. DOI: 10.1287/mnsc.1050.0400

Creazza, A., Colicchia, C., Spiezia, S., & Dallari, F. (2022). Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era. Supply Chain Management: An International Journal, 27(1), 30–53. DOI: 10.1108/SCM-02-2020-0073

Gawer, A. (2014). Bridging differing perspectives on technological platforms. Research Policy, 43(7), 1239–1249. DOI: 10.1016/j.respol.2014.03.006

Kou, G., & Lu, Y. (2025). FinTech: A literature review of emerging financial technologies and applications. Financial Innovation, 11(1), 1–34. DOI: 10.1186/s40854-024-00668-6

Tiwana, A., Konsynski, B., & Bush, A. A. (2010). Platform evolution: Coevolution of platform architecture, governance, and environmental dynamics. Information Systems Research, 21(4), 675–687. DOI: 10.1287/isre.1100.0323

Ivanov, D., & Dolgui, A. (2021). A digital supply chain twin for managing the disruption risks and resilience in the era of Industry 4.0. Production Planning & Control, 32(9), 775–788. DOI: 10.1080/09537287.2020.1768450

Eisenhardt, K. M. (1989). Agency theory: An assessment and review. Academy of Management Review, 14(1), 57–74. DOI: 10.2307/258191

Lu, Y. (2025). The current status and developing trends of Industry 4.0: A review. Information Systems Frontiers, 27(1), 215–234. DOI: 10.1007/s10796-021-10221-w

Boudreau, K. (2010). Open platform strategies and innovation: Granting access vs. devolving control. Management Science, 56(10), 1849–1872. DOI: 10.1287/mnsc.1100.1187

Dubey, R., Gunasekaran, A., Childe, S. J., Fosso Wamba, S., Roubaud, D., & Foropon, C. (2021). Empirical investigation of data analytics capability and organizational flexibility as complements to supply chain resilience. International Journal of Production Research, 59(1), 110–128. DOI: 10.1080/00207543.2019.1582820

Rochet, J. C., & Tirole, J. (2003). Platform competition in two-sided markets. Journal of the European Economic Association, 1(4), 990–1029. DOI: 10.1162/154247603322493212

Wu, H. P., Liu, Z., Dong, H. Y., Lu, Y., & Xu, L. D. (2025). Revolutionizing internal auditing: Harnessing the power of blockchain. Enterprise Information Systems, 19(1–2), 2448003. DOI: 10.1080/17517575.2024.2448003

Constantinides, P., Henfridsson, O., & Parker, G. G. (2018). Introduction—Platforms and infrastructures in the digital age. Information Systems Research, 29(2), 381–400. DOI: 10.1287/isre.2018.0794

Kayan, H., Nunes, M., Rana, O., Burnap, P., & Perera, C. (2022). Cybersecurity of industrial cyber-physical systems: A review. ACM Computing Surveys, 54(11s), 229. DOI: 10.1145/3510410

Gawer, A., & Cusumano, M. A. (2014). Industry platforms and ecosystem innovation. Journal of Product Innovation Management, 31(3), 417–433. DOI: 10.1111/jpim.12105

Xu, L. D., Lu, Y., & Li, L. (2021). Embedding blockchain technology into IoT for security: A survey. IEEE Internet of Things Journal, 8(13), 10452–10473. DOI: 10.1109/JIOT.2021.3060508

Wareham, J., Fox, P. B., & Cano Giner, J. L. (2014). Technology ecosystem governance. Organization Science, 25(4), 1195–1215. DOI: 10.1287/orsc.2014.0895

Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. International Journal of Production Research, 57(7), 2117–2135. DOI: 10.1080/00207543.2018.1533261

Adner, R. (2017). Ecosystem as structure: An actionable construct for strategy. Journal of Management, 43(1), 39–58. DOI: 10.1177/0149206316678451

Lu, Y. (2022). Implementing blockchain in information systems: A review. Enterprise Information Systems, 16(12), 1876–1907. DOI: 10.1080/17517575.2021.2008513

Jacobides, M. G., Cennamo, C., & Gawer, A. (2018). Towards a theory of ecosystems. Strategic Management Journal, 39(8), 2255–2276. DOI: 10.1002/smj.2904

Boyson, S., Corsi, T. M., & Paraskevas, J.-P. (2022). Defending digital supply chains: Evidence from a decade-long research program. Technovation, 118, 102380. DOI: 10.1016/j.technovation.2021.102380

Yoo, Y., Henfridsson, O., & Lyytinen, K. (2010). Research commentary: The new organizing logic of digital innovation. Information Systems Research, 21(4), 724–735. DOI: 10.1287/isre.1100.0322

Zheng, X. R., & Lu, Y. (2022). Blockchain technology: Recent research and future trend. Enterprise Information Systems, 16(12), 1939895. DOI: 10.1080/17517575.2021.1939895

Nambisan, S., Lyytinen, K., Majchrzak, A., & Song, M. (2017). Digital innovation management: Reinventing innovation management research in a digital world. MIS Quarterly, 41(1), 223–238. DOI: 10.25300/MISQ/2017/41:1.03

Ben-Daya, M., Hassini, E., & Bahroun, Z. (2019). Internet of things and supply chain management: A literature review. International Journal of Production Economics, 212, 280–302. DOI: 10.1016/j.ijpe.2017.12.016

Verhoef, P. C., Broekhuizen, T., Bart, Y., Bhattacharya, A., Dong, J. Q., Fabian, N., & Haenlein, M. (2021). Digital transformation: A

multidisciplinary reflection and research agenda. Journal of Business Research, 122, 889–901. DOI: 10.1016/j.jbusres.2019.09.022

Lu, Y., Zheng, X., Li, L., & Xu, L. D. (2020). Pricing the cloud: A QoS-based auction approach. Enterprise Information Systems, 14(3), 334–351. DOI: 10.1080/17517575.2019.1669827

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. Journal of Strategic Information Systems, 28(2), 118–144. DOI: 10.1016/j.jsis.2019.01.003

Baryannis, G., Dani, S., & Antoniou, G. (2019). Predicting supply chain risks using machine learning: The trade-off between performance and interpretability. International Journal of Production Economics, 207, 267–282. DOI: 10.1016/j.ijpe.2018.11.014

Appio, F. P., Frattini, F., Petruzzelli, A. M., & Neirotti, P. (2021). Digital transformation and innovation management: A synthesis of existing research and an agenda for future studies. Journal of Product Innovation Management, 38(1), 4–20. DOI: 10.1111/jpim.12562

Lu, Y., & Xu, L. D. (2019). Internet of Things (IoT) cybersecurity research: A review of current research topics. IEEE Internet of Things Journal, 6(2), 2103–2115. DOI: 10.1109/JIOT.2018.2869847

Plekhanov, D., Franke, H., & Netland, T. H. (2023). Digital transformation: A review and research agenda. European Management Journal, 41(6), 821–844. DOI: 10.1016/j.emj.2022.09.007

Queiroz, M. M., & Fosso Wamba, S. (2019). Blockchain adoption challenges in supply chain: An empirical investigation of the main drivers in India and the USA. International Journal of Information Management, 46, 70–82. DOI: 10.1016/j.ijinfomgt.2018.11.021

Hanelt, A., Bohnsack, R., Marz, D., & Antunes Marante, C. (2021). A systematic review of the literature on digital transformation: Insights and implications for strategy and organizational change. Journal of Management Studies, 58(5), 1159–1197. DOI: 10.1111/joms.12639

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

Hein, A., Schreieck, M., Riasanow, T., Setzke, D. S., Wiesche, M., Bohm, M., & Krcmar, H. (2020). Digital platform ecosystems. Electronic Markets, 30(1), 87–98. DOI: 10.1007/s12525-019-00377-4

Wamba, S. F., Gunasekaran, A., Akter, S., Ren, S. J.-F., Dubey, R., & Childe, S. J. (2017). Big data analytics and firm performance: Effects of dynamic capabilities. Journal of Business Research, 70, 356–365. DOI: 10.1016/j.jbusres.2016.08.009

Rai, A., Patnayakuni, R., & Seth, N. (2006). Firm performance impacts of digitally enabled supply chain integration capabilities. MIS Quarterly, 30(2), 225–246. DOI: 10.2307/25148729

Kouhizadeh, M., Saberi, S., & Sarkis, J. (2021). Blockchain technology and the sustainable supply chain: Theoretically exploring adoption barriers. International Journal of Production Economics, 231, 107831. DOI: 10.1016/j.ijpe.2020.107831

Belhadi, A., Kamble, S., Jabbour, C. J. C., Gunasekaran, A., Ndubisi, N. O., & Venkatesh, M. (2021). Manufacturing and service supply chain resilience to the COVID-19 outbreak: Lessons learned from the automobile and airline industries. Technological Forecasting and Social Change, 163, 120447. DOI: 10.1016/j.techfore.2020.120447

Park, A., & Li, H. (2021). The effect of blockchain technology on supply chain sustainability performances. Sustainability, 13(4), 1726. DOI: 10.3390/su13041726

Ivanov, D. (2020). Predicting the impacts of epidemic outbreaks on global supply chains. Transportation Research Part E: Logistics and Transportation Review, 136, 101922. DOI: 10.1016/j.tre.2020.101922

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics, 36, 55–81. DOI: 10.1016/j.tele.2018.11.006

Ivanov, D. (2022). Viable supply chain model: Integrating agility, resilience and sustainability perspectives—lessons from and thinking beyond the COVID-19 pandemic. Annals of Operations Research, 319, 1411–1431. DOI: 10.1007/s10479-020-03640-6

Boyson, S. (2014). Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems. Technovation, 34(7), 342–353. DOI: 10.1016/j.technovation.2014.02.001

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

Zhang, C., & Lu, Y. (2021). Study on artificial intelligence: The state of the art and future prospects. Journal of Industrial Information Integration, 23, 100224. DOI: 10.1016/j.jii.2021.100224

Tang, C. S. (2006). Robust strategies for mitigating supply chain disruptions. International Journal of Logistics Research and Applications, 9(1), 33–45. DOI: 10.1080/13675560500405584

Yaacoub, J. P. A., Salman, O., Noura, H. N., Kaaniche, N., Chehab, A., & Malli, M. (2020). Cyber-physical systems security: Limitations, issues and future trends. Microprocessors and Microsystems, 77, 103201. DOI: 10.1016/j.micpro.2020.103201

Wieland, A., & Wallenburg, C. M. (2012). Dealing with supply chain risks: Linking risk management practices and strategies to performance. International Journal of Physical Distribution & Logistics Management, 42(10), 887–905. DOI: 10.1108/09600031211281411

Yu, Z., Gao, H., Cong, X., Wu, N., & Song, H. H. (2023). A survey on cyber-physical systems security. IEEE Internet of Things Journal, 10(24), 21670–21686. DOI: 10.1109/JIOT.2023.3289625

Jüttner, U., Peck, H., & Christopher, M. (2003). Supply chain risk management: Outlining an agenda for future research. International Journal of Logistics Research and Applications, 6(4), 197–210. DOI: 10.1080/1367556031000162701 6

Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security—A survey. IEEE Internet of Things Journal, 4(6), 1802–

1831. DOI: 10.1109/JIOT.2017.2703172

Ani, U. P. D., He, H., & Tiwari, A. (2017). Review of cybersecurity issues in industrial critical infrastructure: Manufacturing in perspective. Journal of Cyber Security Technology, 1(1), 32–74. DOI: 10.1080/23742917.2016.1252211

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

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. DOI: 10.1177/1461444816676645

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

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. DOI: 10.1177/2053951716679679

Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. Nature Machine Intelligence, 1, 389–399. DOI: 10.1038/s42256-019-0088-2

Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., & Vayena, E. (2018). AI4People—An ethical framework for a good AI society. Minds and Machines, 28, 689–707. DOI: 10.1007/s11023-018-9482-5

Rai, A. (2020). Explainable AI: From black box to glass box. Journal of the Academy of Marketing Science, 48(1), 137–141. DOI: 10.1007/s11747-019-00710-5

Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). Why should I trust you? Explaining the predictions of any classifier. Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 1135–1144. DOI: 10.1145/2939672.2939778

Lundberg, S. M., & Lee, S. I. (2017). A unified approach to interpreting model predictions. Advances in Neural Information Processing Systems, 30. DOI: 10.48550/arXiv.1705.07874

Doshi-Velez, F., & Kim, B. (2017). Towards a rigorous science of interpretable machine learning. arXiv preprint. DOI: 10.48550/arXiv.1702.08608

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. Proceedings of the ACM Conference on Fairness, Accountability, and Transparency, 33–44. DOI: 10.1145/3351095.3372873

Selbst, A. D., Boyd, D., Friedler, S. A., Venkatasubramanian, S., & Vertesi, J. (2019). Fairness and abstraction in sociotechnical systems. Proceedings of the ACM Conference on Fairness, Accountability, and Transparency, 59–68. DOI: 10.1145/3287560.3287598

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. DOI: 10.1093/idpl/ipx005

Barocas, S., & Selbst, A. D. (2016). Big Data's disparate impact. California Law Review, 104(3), 671–732. DOI: 10.15779/Z38BG31

Kizilcec, R. F. (2016). How much information? Effects of transparency on trust in an algorithmic interface. Proceedings of the CHI Conference on Human Factors in Computing Systems, 2390–2395. DOI: 10.1145/2858036.2858402

Eslami, M., Rickman, A., Vaccaro, K., Aleyasen, A., Vuong, A., Karahalios, K., Hamilton, K., & Sandvig, C. (2015). “I always assumed that I wasn't really that close to [her]”: Reasoning about invisible algorithms in news feeds. Proceedings of the CHI Conference on Human Factors in Computing Systems, 153–162. DOI: 10.1145/2702123.2702556

Lee, M. K. (2018). Understanding perception of algorithmic decisions: Fairness, trust, and emotion in response to algorithmic management. Big Data & Society, 5(1), 1–16. DOI: 10.1177/2053951718756684

Rahwan, I. (2018). Society-in-the-loop: Programming the algorithmic social contract. Ethics and Information Technology, 20(1), 5–14. DOI: 10.1007/s10676-017-9430-8

Kellogg, K. C., Valentine, M. A., & Christin, A. (2020). Algorithms at work: The new contested terrain of control. Academy of Management Annals, 14(1), 366–410. DOI: 10.5465/annals.2018.0174

Jarrahi, M. H., Newlands, G., Lee, M. K., Wolf, C. T., Kinder, E., & Sutherland, W. (2021). Algorithmic management in a work context. Big Data & Society, 8(2), 1–14. DOI: 10.1177/20539517211020332

Parent-Rocheleau, X., & Parker, S. K. (2022). Algorithms as work designers: How algorithmic management influences the design of jobs. Human Resource Management Review, 32(3), 100838. DOI: 10.1016/j.hrmr.2021.100838

Martin, K. (2019). Ethical implications and accountability of algorithms. Journal of Business Ethics, 160(4), 835–850. DOI: 10.1007/s10551-018-3921-3

Mahmud, H., Islam, A. K. M. N., Ahmed, S. I., & Smolander, K. (2022). What influences algorithmic decision-making? A systematic literature review on algorithm aversion. Technological Forecasting and Social Change, 175, 121390. DOI: 10.1016/j.techfore.2021.121390