



DFAS-EconomyGov: A Conceptual Governance Doctrine for Algorithmic Market Integrity and Supply Chain Resilience

Hasan Mohamed Husain Alaali*
DFAS Research Center, Kingdom of Bahrain

Received : May 15, 2026

Revised : June 21, 2026

Accepted : August 10, 2026

Online : October 21, 2026

Abstract

Artificial intelligence (AI) is increasingly embedded in financial markets, trade, and supply-chain decision systems, creating opportunities for efficiency and resilience while introducing governance problems involving opacity, algorithmic interaction, technological dependence, supply-chain fragility, and jurisdictional misalignment. Existing governance approaches address important elements of AI ethics, risk management, accountability, regulation, and resilience, but these functions remain only partially integrated within economically consequential AI-mediated decisions. This study employs a non-empirical doctrinal and conceptual design approach. Evidence from peer-reviewed research, regulatory and institutional publications, and international standards is synthesized to identify recurring governance problems and derive corresponding requirements. These requirements are translated into a governance doctrine and evaluated through evidence-based comparative analysis and three illustrative conceptual scenarios, including a failure-oriented stress scenario. The scenarios demonstrate conceptual operation and boundaries rather than empirical validation. The study develops DFAS-EconomyGov, centered on the Alaali Economy Governance Doctrine (A-EGD) and operationalized through four supporting functions: explainability escalation (A-MEEF), authority-bounded intervention (A-TOCC), jurisdiction-sensitive calibration (A-SCETM), and optional governance traceability (A-MIL). Comparative analysis indicates that established instruments provide substantial coverage of individual governance functions, while DFAS-EconomyGov differs primarily in their configuration. Scenario analysis identifies applicability boundaries arising from poorly calibrated intervention, conflicting jurisdictional requirements, and insufficient technical or contractual control over third-party AI systems. The contribution is configurational rather than elemental: DFAS-EconomyGov connects detection and explainability to escalation, intervention authority, jurisdiction-sensitive calibration, and traceability within a single economic governance doctrine. The study establishes conceptual structure, comparative positioning, and identifiable failure conditions, but not empirical effectiveness or superiority.

Keywords: *AI Governance, Algorithmic Market Integrity, Supply-Chain Resilience, Economic Sovereignty, DFAS-EconomyGov.*

INTRODUCTION

Algorithmic Transformation of Markets and Supply Chains

Artificial intelligence (AI) is becoming embedded in the operational infrastructure of financial markets, trade, and supply chains. In capital markets, AI and machine-learning systems increasingly support trading, portfolio management, surveillance, and risk assessment. The International Monetary Fund identifies expanding AI adoption as potentially consequential for market structure, trading strategies, volatility, and financial stability (IMF, 2024). Financial authorities similarly recognize AI's growing role in analytics, risk management, operational processes, and decision-making across financial services (Crisanto et al., 2024; FSB, 2024).

This transformation extends to demand forecasting, procurement, inventory management, logistics, and disruption management. AI can strengthen supply-chain resilience through improved



visibility, forecasting, agility, and adaptive capacity (Belhadi et al., 2023; Dey et al., 2023). The World Trade Organization further identifies AI as a potential driver of lower trade costs, productivity growth, and expanded market access while emphasizing the importance of domestic policy and international cooperation (WTO, 2025). AI-mediated decisions therefore increasingly connect goods, capital, information, institutions, and jurisdictions within a shared economic decision environment.

Emerging Governance Risks

The same transformation creates governance problems characterized by speed, opacity, interaction effects, technological dependence, and distributed authority. Autonomous pricing algorithms can learn strategies producing sustained supra-competitive outcomes without explicit human coordination (Calvano et al., 2020). Automated market interactions can also contribute to instability within timescales that constrain conventional intervention, as illustrated by evidence from the Flash Crash (Kirilenko et al., 2017).

More recent assessments identify additional concerns involving opacity, cyber vulnerability, common models and datasets, concentrated third-party providers, correlated behavior, and potential market instability (IMF, 2024; FSB, 2024). Supply chains present a related tension: AI can improve resilience and efficiency while increasing dependence on algorithmic optimization and technological infrastructure (Belhadi et al., 2023; Dey et al., 2023).

These developments create a governance problem that extends beyond identifying AI risk. Institutions must determine when anomalous or insufficiently explainable decisions require escalation, who possesses legitimate authority to intervene, what controls are technically available, how cross-jurisdictional requirements affect decisions, and how consequential governance actions remain attributable and reviewable.

Research Problem and Governance Gap

The research problem is not an absence of AI governance. The OECD AI Principles establish normative expectations for trustworthy and accountable AI (OECD, 2024); the NIST AI Risk Management Framework structures organizational AI risk management (Tabassi, 2023); Regulation (EU) 2024/1689 establishes binding requirements within its legal scope (European Parliament & Council of the European Union, 2024); and financial authorities address governance, model risk, third-party dependencies, and supervisory capacity (Crisanto et al., 2024; FSB, 2024). Established governance theory also provides important foundations. Responsive regulation addresses graduated and context-sensitive intervention (Ayres & Braithwaite, 1992); meta-regulation emphasizes governance of organizational control processes (Parker, 2002); polycentric governance recognizes distributed centres of authority (Ostrom, 2010); and accountability theory emphasizes answerability, scrutiny, and consequences (Bovens, 2007). AI-governance scholarship nevertheless continues to identify difficulties in translating principles and governance requirements into organizational practice (Mäntymäki et al., 2022; Herzog et al., 2023).

The gap identified in this study is therefore configurational rather than elemental. Existing scholarship and instruments address explainability, risk management, oversight, accountability, resilience, regulation, and jurisdiction through different governance streams. What remains insufficiently integrated is the connection among explainability-linked escalation, authority-bounded intervention, jurisdiction-sensitive calibration, and traceability within AI-mediated economic decisions spanning markets, trade, and supply chains.

This is a bounded gap claim. It does not imply that existing instruments are deficient or that no institution combines similar functions in practice. Rather, it identifies an unresolved integration problem that provides the basis for the doctrinal construction developed in this study.

Research Objective and Research Question

This study addresses the identified gap by developing and conceptually evaluating DFAS-EconomyGov, a governance doctrine for AI-mediated financial markets, trade processes, and supply-chain infrastructures. The study examines how governance requirements identified independently from the literature can be translated into connected operational functions while remaining bounded by legitimate authority, technological access, and institutional accountability. The research question is:

“How can a jurisdiction-sensitive governance doctrine integrate explainability escalation, authority-bounded intervention, calibration, and traceability to support algorithmic market integrity and supply-chain resilience?”

The objective is to construct the doctrine, derive its governance functions from the identified problems, compare its functional configuration with established governance instruments, and examine its conceptual applicability and failure boundaries through illustrative scenarios. The study does not test empirical effectiveness or claim legal enforceability.

Contribution and Paper Organization

The study advances **one central contribution**: the construction of an integrated economic AI governance doctrine connecting explainability and detection to escalation, escalation to governed intervention, cross-border operation to jurisdiction-sensitive calibration, and consequential governance actions to traceability and review.

Dynamic Financial Applied Meta-Science (DFAS) provides the broader meta-scientific foundation within which DFAS-EconomyGov is developed. DFAS-EconomyGov extends antecedent DFAS research on embedded governance, institutional deployment, and jurisdiction-sensitive financial AI governance (Alaali, 2025a, 2025b, 2026), while positioning that contribution within independent governance and AI-governance literature rather than relying on self-citation as its theoretical foundation.

Its normative core is the Alaali Economy Governance Doctrine (A-EGD). Four supporting mechanisms translate the doctrine into identifiable governance functions: the Alaali Market Explainability Escalation Framework (A-MEEF), Alaali Trade Override Command Chain (A-TOCC), Alaali Sovereign Calibration Engine for Trade & Markets (A-SCETM), and optional Alaali Market Integrity Ledger (A-MIL). These mechanisms are operational expressions of the central doctrine rather than separate theoretical contributions.

The remainder of the paper reviews the theoretical and empirical literature, specifies the doctrinal and conceptual methodology, presents the findings and architecture, evaluates its comparative positioning and conceptual failure boundaries, and concludes with limitations and directions for empirical testing.

LITERATURE REVIEW

AI Governance: From Principles to Operational Control

Contemporary AI governance encompasses normative principles, organizational risk management, technical controls, and legally binding regulation. The OECD AI Principles provide an international normative baseline emphasizing trustworthy AI, transparency, robustness, human-centred values, and accountability (OECD, 2024). The NIST Artificial Intelligence Risk Management Framework (AI RMF 1.0) provides a voluntary and non-sector-specific structure organized around Govern, Map, Measure, and Manage functions (Tabassi, 2023), while Regulation (EU) 2024/1689 establishes binding obligations for AI systems falling within its jurisdictional and risk-based scope (European Parliament & Council of the European Union, 2024).

These instruments represent different governance modalities rather than interchangeable alternatives. Principles articulate normative expectations; risk-management systems organize institutional processes; and regulation establishes legally enforceable obligations. The relevant question for the present study is therefore not whether AI governance exists, but how governance requirements are translated into decision-level controls when AI participates materially in economically consequential activity.

This implementation problem is well established in the literature. [Mäntymäki et al. \(2022\)](#), in a systematic review of organizational AI governance, identify limited understanding of implementation, contextual conditions, regulatory effectiveness, and the operationalization of governance processes. [Mittelstadt \(2019\)](#) similarly argues that high-level AI ethics principles face substantial limitations when translated into organizational practice because principles alone do not resolve conflicts among values, establish institutional incentives, or determine responsibility for implementation. More recent scholarship continues to characterize the transition from principles to practice as a substantive governance problem rather than a purely technical implementation task ([Hagendorff, 2020](#); [Herzog et al., 2023](#); [Prem, 2025](#)).

The problem is especially consequential in financial systems. Financial authorities identify model risk, data governance, cyber vulnerability, third-party dependencies, concentration, skills, accountability, and supervisory capacity as material governance concerns accompanying greater AI adoption ([Crisanto et al., 2024](#); [FSB, 2024](#)). Governance in this setting therefore requires more than ethical guidance or ex ante risk identification. It must also address how concerns are detected, escalated, reviewed, acted upon, documented, and reassessed as systems and operating conditions change.

This distinction is consistent with broader governance theory. Responsive regulation emphasizes that regulatory intervention should vary according to conduct, context, and the capacity of regulated actors rather than depend exclusively on uniform ex ante commands ([Ayres & Braithwaite, 1992](#)). Meta-regulation shifts attention toward the governance of organizations' own internal risk-management and control processes while retaining external accountability ([Parker, 2002](#)). Polycentric governance further recognizes that complex governance problems may involve multiple overlapping centres of decision authority rather than a single hierarchical controller ([Ostrom, 2010](#)). These perspectives differ in origin and purpose, but collectively indicate that effective governance may require adaptation, distributed authority, escalation, and accountability rather than static rule articulation alone.

Recent AI-governance research reinforces this point. [Kleiner \(2026\)](#) conceptualizes AI governance through interacting operational and societal feedback loops and argues that distributed authority and reflexive checkpoints are important where governance and AI-mediated decision processes continuously affect one another. Empirical evidence from public organizations likewise indicates that AI-governance implementation depends on combinations of organizational processes, institutional standards, training, stakeholder roles, and operational practices rather than the mere existence of ethical principles ([Almeida & dos Santos Júnior, 2024](#)).

These theoretical and empirical perspectives provide an external foundation for the present study. Antecedent DFAS research contributes additional reasoning concerning embedded governance and institutional deployment ([Alaali, 2025a, 2025b](#)), but it is treated here as intellectual lineage rather than independent validation evidence. The unresolved question is more specific: how governance functions can be configured around economically consequential AI decisions that simultaneously implicate market integrity, intervention authority, cross-border jurisdiction, resilience, and accountability.

Algorithmic Market Integrity and Financial-System Risk

AI-mediated markets create governance problems through speed, opacity, interaction effects, strategic adaptation, interconnectedness, and potentially systemic consequences. These characteristics can weaken governance arrangements that depend on retrospective explanation or discretionary intervention occurring only after harmful behavior has become observable.

The 2010 Flash Crash provides an important empirical illustration of the temporal dimension of automated markets. [Kirilenko et al. \(2017\)](#) show how interactions among high-frequency market participants contributed to market dynamics during an episode of extreme instability. Although the Flash Crash predates contemporary generative AI and should not be interpreted as evidence about current AI systems generally, it demonstrates the governance significance of automated interactions occurring at speeds that constrain conventional human response.

Algorithmic pricing presents a distinct but related problem. Experimental evidence shows that autonomous pricing algorithms can learn strategies producing sustained supra-competitive outcomes without explicit communication among human principals ([Calvano et al., 2020](#)). This complicates conventional assumptions linking harmful market coordination to identifiable human communication or intent. The governance problem therefore extends from detecting undesirable outcomes to determining how anomalous algorithmic behavior should be investigated, attributed, challenged, contained, and reviewed.

As AI diffuses across financial institutions and market infrastructures, the risk perimeter broadens. The International Monetary Fund ([IMF, 2024](#)) identifies potential implications for market structure, trading strategies, volatility, opacity, and financial stability. The Financial Stability Board ([FSB, 2024](#)) additionally identifies third-party dependencies, cyber risks, common models and datasets, technological concentration, and correlated behavior as potential sources of systemic vulnerability. These concerns demonstrate that governance may fail even when an individual model performs as designed: common infrastructure, providers, datasets, or optimization strategies can generate dependencies extending beyond a single institution.

Generative AI adds an information-governance dimension. Unlike systems primarily executing predefined optimization or trading functions, generative systems can produce recommendations, interpretations, assessments, synthetic information, and other outputs capable of entering economically consequential decision processes. Their governance significance therefore depends not simply on whether generative AI is present but on whether its outputs materially influence decisions concerning markets, investment, procurement, logistics, risk, or institutional action. Where they do, questions of reliability, attribution, contestability, escalation, and decision authority become relevant.

These issues intersect with accountability theory. [Bovens \(2007\)](#) conceptualizes accountability as a relationship in which an actor is obliged to explain and justify conduct to a forum capable of questioning and judging that conduct and imposing consequences. Applied to AI-mediated economic decisions, accountability cannot be reduced to the availability of technical explanation. It also requires identifiable responsibility, legitimate authority to challenge or intervene, and records sufficient to reconstruct consequential governance actions.

Algorithmic auditing provides another adjacent governance mechanism. Internal algorithmic auditing can structure examination of AI systems across the development and deployment lifecycle and generate documentation that supports organizational accountability ([Raji et al., 2020](#)). Ethics-based auditing similarly provides a structured mechanism for assessing automated decision-making systems against relevant principles or norms and can strengthen procedural regularity and transparency, while remaining subject to conceptual, technical, organizational, and institutional limitations ([Mökander et al., 2021](#)). Auditing can therefore make

otherwise opaque processes more inspectable and support accountability, but it does not by itself determine who possesses legitimate authority to suspend, modify, reject, or otherwise intervene in an economically consequential AI-mediated decision. This distinction between audit-based visibility and intervention authority is central to the governance configuration developed in this study.

The literature consequently supports a multi-stage governance problem: economically consequential algorithmic behavior must be detectable; its materiality must be assessable; relevant actors must possess legitimate and technically feasible authority to respond; intervention itself must remain accountable; and subsequent decisions must be reviewable. This problem structure provides the market-integrity basis for the later derivation of explainability escalation, governed intervention, and traceability requirements rather than presuming those mechanisms in advance.

AI, Trade, and Supply-Chain Resilience

AI is increasingly used to support demand forecasting, inventory management, procurement, logistics, disruption detection, visibility, coordination, and supply-chain adaptation. Research generally identifies substantial potential for AI to strengthen resilience by improving information processing and enabling faster responses to uncertainty and disruption (Belhadi et al., 2023; Dey et al., 2023; Singh et al., 2025; Sunmola & Baryannis, 2024).

The evidence nevertheless cautions against equating optimization capability with resilience. Dey et al. (2023), using evidence from Vietnamese manufacturing SMEs, demonstrate that AI-enabled capabilities can contribute to supply-chain resilience, but organizational and contextual conditions influence how those capabilities are translated into resilience outcomes. Belhadi et al. (2023) similarly identify multiple mechanisms through which AI can support readiness, response, recovery, and adaptation while emphasizing continuing research requirements surrounding implementation and resilience capabilities.

Importantly, primary research also identifies conditions under which AI-mediated supply-chain decisions can generate adverse outcomes. Li and Li (2022), examining AI automation of retailer ordering decisions in a decentralized supply chain, demonstrate that automation does not necessarily improve supply-chain outcomes. Under particular economic and behavioral conditions, AI automation can operate as a negative force and can produce a lose-lose outcome in which both the retailer and supplier are worse off. Their analysis therefore provides direct evidence that automating an individually rational supply-chain decision does not guarantee system-level improvement and that the consequences of AI-mediated decisions depend on the surrounding incentive and coordination structure.

More recent empirical evidence identifies a different form of supply-chain exposure. Dong et al. (2026), using an event-study design and configurational analysis, examine AI ethics incidents affecting publicly listed U.S. firms and show that adverse consequences can extend beyond the focal organization to customer firms connected through supply-chain relationships. This evidence demonstrates that AI-related failures need not remain localized within the organization deploying or developing the technology; their effects can propagate across interorganizational dependencies. Together, these studies strengthen the risk side of the evidence base. They indicate two distinct governance problems relevant to the present study: AI-mediated decisions can generate adverse outcomes within decentralized supply-chain relationships, and AI-related failures can transmit consequences across supply-chain connections. The governance issue is therefore not simply whether AI improves average efficiency or resilience, but whether institutions can detect and respond when locally optimized or technologically mediated decisions create wider economic consequences.

Supply-chain research also demonstrates why efficiency-oriented arrangements may become vulnerable under severe disruption. [Craighead et al. \(2020\)](#) show that major disruptions can expose structural dependencies and vulnerabilities that conventional efficiency assumptions inadequately accommodate. Related research emphasizes that multi-stakeholder collaboration and governance arrangements can contribute to broader economic resilience ([Buasan et al., 2026](#)). The governance implication is important: an AI recommendation can remain internally consistent with its optimization objective while becoming inappropriate after disruption alters legal constraints, resource availability, risk tolerance, or continuity priorities.

AI-mediated supply chains therefore create a distinction between algorithmic optimization and governed resilience. Forecast accuracy, routing efficiency, inventory minimization, or procurement cost may be legitimate objectives under ordinary conditions, but they do not automatically determine the appropriate response under sanctions, border restrictions, infrastructure failure, geopolitical disruption, or critical-resource scarcity. Governance requires institutional capacity to identify when the decision environment has materially changed and to determine whether existing algorithmic objectives or constraints remain acceptable.

ISO 28000:2022 provides a relevant management-system reference for supply-chain security and resilience, but it is not an AI-specific governance architecture ([ISO, 2022](#)). The [WTO \(2025\)](#), meanwhile, identifies AI's potential to reduce trade costs, increase productivity, and expand market access while emphasizing the importance of domestic policy, international cooperation, and the regulatory environment. These instruments therefore address significant components of the problem without resolving how AI-mediated supply-chain decisions should be escalated and governed when optimization, resilience, regulatory compliance, and public-policy requirements diverge.

This literature also cautions against assuming that additional technical control necessarily solves the principles-to-practice problem. Critical scholarship argues that reducing AI governance to technical implementation can neglect institutional, social, ethical, and power relationships surrounding deployment ([Prem, 2025](#)). For supply chains, this means that governance must concern not only the algorithm but also organizations, technology providers, regulators, contractual relationships, decision authority, and actors affected by operational choices.

The resulting governance problem is therefore conditional rather than categorical. AI can strengthen resilience, but empirical and analytical evidence demonstrates that AI-mediated decisions can also produce adverse outcomes or transmit risks through supply-chain relationships under particular conditions. What remains insufficiently specified is how institutions should govern the transition from ordinary algorithmic optimization to heightened scrutiny, intervention, or recalibration when operating conditions materially change.

Economic Sovereignty and Jurisdictional Calibration

Cross-border AI-mediated economic systems operate across jurisdictions characterized by different laws, regulatory institutions, market structures, trade obligations, technological capabilities, and public-policy priorities. Cross-border economic integration therefore does not eliminate jurisdictional heterogeneity; it creates additional interfaces through which heterogeneous requirements must be reconciled ([Abbassy et al., 2025](#)).

Digital-sovereignty scholarship provides an important conceptual distinction between legitimate political or legal authority and practical technological control. [Roberts \(2024\)](#) argues that digital sovereignty involves normative questions concerning authority and control rather than merely technological autonomy. This distinction is central to AI-mediated economic governance because an institution or state may possess formal legal authority while lacking direct control over the technological infrastructure through which AI decisions are generated.

Such constraints are increasingly material where organizations depend on externally controlled cloud services, proprietary foundation models, application programming interfaces, externally hosted datasets, specialized computing infrastructure, or concentrated technology providers. The [FSB \(2024\)](#) identifies third-party dependencies and technological concentration as relevant financial-stability concerns. Formal authority to require a governance outcome therefore does not establish that the implementing institution possesses model-level or parameter-level access necessary to produce it.

Three concepts should consequently be distinguished. Legal sovereignty concerns legitimate jurisdictional authority to establish or enforce applicable requirements. Technological capacity concerns the practical ability to implement, verify, constrain, suspend, substitute, or otherwise govern technological systems. Legitimate intervention authority concerns which institution or actor is authorized to exercise a particular governance action under applicable institutional and legal arrangements. Conflating these dimensions risks attributing operational power to actors that possess formal authority but insufficient technical access.

This distinction also establishes a technical-access boundary for jurisdictional calibration. Where an institution operates a closed-source third-party AI service, governance may realistically occur at the output, workflow, procurement, contractual, audit, deployment, or suspension level rather than through direct alteration of source code, training data, model weights, or internal parameters. Jurisdiction-sensitive governance must therefore adapt to the level of control actually available rather than assume unrestricted technical sovereignty.

Regulatory fragmentation creates an additional problem. Regulation (EU) 2024/1689 establishes a harmonized AI regime within the European Union, whereas AI-mediated markets and supply chains can simultaneously interact with non-EU legal regimes, trade obligations, sanctions, data rules, and sector-specific requirements. The [WTO \(2025\)](#) likewise emphasizes interactions among AI-enabled trade, domestic policy, regulatory fragmentation, and international cooperation. Cross-border governance can therefore involve both technological dependence and overlapping or conflicting jurisdictional obligations.

Polycentric governance provides one theoretical lens for understanding this environment because authority can be distributed across regulators, market authorities, firms, technology providers, courts, standard setters, and international institutions rather than concentrated within one decision centre ([Ostrom, 2010](#)). Recent AI-governance scholarship similarly emphasizes interactions among operational deployment, societal oversight, distributed authority, and institutional context ([Kleiner, 2026](#)). These perspectives caution against treating sovereignty as a unilateral command mechanism.

Accordingly, jurisdictional calibration in the present study does not mean automatic compliance with every instruction issued by a public authority. Applicable law, institutional mandate, conflicts of jurisdiction, accountability, technological feasibility, and the legitimacy of intervention remain analytically distinct questions. Nor can a governance architecture itself resolve competing sovereign claims. It can identify, differentiate, document, and escalate conflicts; substantive resolution may require conflict-of-laws rules, treaties, regulatory coordination, judicial determination, or political negotiation.

Theoretical Foundations and Alternative Governance Perspectives

The governance problem developed above intersects with several established theoretical traditions rather than originating exclusively within DFAS. Five are particularly relevant.

First, responsive regulation emphasizes graduated and context-sensitive intervention rather than reliance on a single regulatory response ([Ayres & Braithwaite, 1992](#)). This provides theoretical support for escalation logic but does not itself specify an AI-specific economic

intervention architecture.

Second, meta-regulation emphasizes governance of organizations' internal systems for managing risk and compliance (Parker, 2002). This is relevant because AI governance depends partly on whether institutions establish internal responsibility, monitoring, review, and control processes. However, meta-regulation does not by itself resolve the speed, technical-access, or cross-jurisdictional problems created by AI-mediated economic decisions.

Third, polycentric governance recognizes multiple centres of authority operating through overlapping and interacting arrangements (Ostrom, 2010). This is particularly relevant to cross-border markets and supply chains, where regulators, firms, technology providers, standard setters, auditors, and public authorities possess different forms of authority and capability. Polycentricity nevertheless creates its own coordination and accountability problems rather than guaranteeing effective governance.

Fourth, accountability theory distinguishes accountability from general responsibility by emphasizing answerability, justification, scrutiny, and consequences (Bovens, 2007). This provides a theoretical basis for requiring consequential interventions to remain attributable and reviewable. Accountability, however, does not alone determine when intervention should occur or how jurisdictional constraints should modify AI-mediated decisions.

Fifth, configurational theory provides the theoretical basis for the study's configurational contribution. Configurational reasoning emphasizes that analytically meaningful outcomes may depend on how multiple elements are combined and interact rather than on the independent contribution of individual elements (Fiss, 2007). Applied here, the contribution does not depend on explainability, escalation, intervention, jurisdictional calibration, or traceability being individually novel. It lies in configuring these established governance functions as an integrated sequence in which each performs a distinct but interdependent role. Accordingly, DFAS-EconomyGov advances a configurational rather than elemental contribution.

These perspectives also expose alternatives to the governance configuration developed in this study. Governance could rely more heavily on ex ante authorization, legal liability, external auditing, organizational risk management, market discipline, vendor obligations, or supervisory enforcement rather than embedded intervention mechanisms. Each may be appropriate under particular conditions. For example, liability can allocate consequences after harm; authorization can constrain deployment before operation; auditing can increase visibility; and procurement or contractual controls can govern third-party providers where direct model access is unavailable.

The present study therefore does not assume that embedded operational intervention is universally preferable. Its narrower proposition is that environments characterized simultaneously by algorithmic speed, material economic consequences, technological dependence, and jurisdictional heterogeneity create a governance problem that purely ex ante or retrospective mechanisms may not completely address. Whether the proposed configuration adds value relative to alternative combinations remains an empirical question.

This theoretical positioning also clarifies the role of antecedent DFAS scholarship. Prior DFAS research contributes the intellectual lineage of embedded governance, deployment-oriented governance, and jurisdiction-sensitive financial AI governance (Alaali, 2025a, 2025b, 2026). These works inform doctrinal construction but do not constitute independent evidence that the resulting architecture is valid or superior. External governance theory and independent AI-governance literature establish the disciplinary context within which the present contribution is positioned.

Literature Synthesis and Identified Gap

The literature establishes substantial progress across trustworthy AI, organizational AI governance, risk management, legal regulation, accountability, algorithmic markets, supply-chain

resilience, digital sovereignty, and international trade. It therefore does not support a claim that the individual elements underlying DFAS-EconomyGov are absent from existing scholarship.

The synthesis instead indicates that these established bodies of scholarship address partially connected governance functions rather than a single integrated economic AI governance configuration.

Table 1. Summary of Principal Relationships Identified in the Literature

Existing literature addresses	Remaining problem examined in this study
Trustworthy-AI principles and ethics	Translation of principles into decision-level economic governance processes
Organizational AI risk management	Connection between risk identification, escalation, and consequential intervention
Algorithmic-market competition risks	Governance of anomalous or harmful AI-mediated market behavior at operational speed
Explainability and transparency	Connection between insufficient explanation or contestability and governance consequence
Human oversight	Specification of authorized, constrained, and accountable intervention authority
Algorithmic auditing and accountability	Traceability across detection, escalation, intervention, recalibration, and review
Supply-chain resilience	Governance of algorithmic optimization when resilience, compliance, and efficiency diverge
Digital sovereignty	Distinction between formal authority and actual technological control
International trade and AI policy	Adaptation to heterogeneous and potentially conflicting jurisdictional requirements
Polycentric and multi-level governance	Coordination of distributed authority within AI-mediated economic decision processes

The gap identified from this synthesis is therefore configurational rather than elemental. Explainability, oversight, auditing, resilience, accountability, risk management, regulation, and sovereignty are already developed in different bodies of scholarship. The unresolved issue concerns how these functions can be connected when an AI-mediated economic decision requires detection and explanation, escalation according to materiality, legitimate intervention authority, jurisdiction-sensitive calibration, and traceability of consequential governance actions.

This claim is deliberately bounded. The literature reviewed does not establish that no institution or governance arrangement already combines some or all of these functions in practice. Nor does the absence of an identical published configuration demonstrate the superiority of DFAS-EconomyGov. Rather, the reviewed literature indicates that these functions are generally theorized, regulated, or operationalized through partially separate governance streams and instruments.

The configurational gap can therefore be represented as:

Detection and Explainability → Escalation → Authorized Intervention → Jurisdiction-Sensitive Calibration → Traceability and Review

The significance of this configuration lies in connecting governance functions across both algorithmic markets and AI-mediated trade and supply-chain systems rather than proposing each constituent function as independently novel.

This configuration also creates an analytically testable proposition. If integration has value beyond the individual governance elements, subsequent empirical research should be able to determine whether institutions implementing connected escalation, intervention, calibration, and traceability processes exhibit different governance outcomes from institutions deploying these controls independently. Conversely, evidence that existing arrangements perform equally well, or that integration produces excessive cost, latency, conflict, or complexity, would weaken the claimed incremental value of the configuration.

The present study builds on antecedent DFAS work concerning embedded governance (Alaali, 2025b), institutional deployment (Alaali, 2025a), and jurisdiction-sensitive financial AI governance (Alaali, 2026), but narrows the contribution to one central proposition: economically consequential AI may benefit from an integrated governance configuration linking explanation and detection to escalation, legitimate intervention, jurisdiction-sensitive calibration, and accountable traceability.

The four recurring governance problems used to derive the corresponding governance requirements are operationally identified in the Methodology section under the predefined recurrence criterion and are not restated here. DFAS-EconomyGov is developed as the governance doctrine responding to the resulting configurational problem. The Alaali Economy Governance Doctrine (A-EGD) constitutes its normative core, while A-MEEF, A-TOCC, A-SCETM, and A-MIL specify supporting governance functions rather than independent theoretical contributions. Their derivation and conceptual evaluation are specified in the methodology that follows.

RESEARCH METHODS

Research Design: Doctrinal and Conceptual Design Approach

This study adopts a non-empirical doctrinal and conceptual design approach to construct and conceptually evaluate an economic AI governance doctrine rather than test statistical hypotheses or empirical effectiveness. Conceptual research can integrate constructs, specify relationships, and develop alternative explanatory structures (MacInnis, 2011), while disciplined theory construction requires explicit problem specification and evaluation beyond novelty alone (Weick, 1989). Design-oriented reasoning further supports knowledge development through purposeful conceptual artifacts (Hevner et al., 2004).

DFAS-EconomyGov constitutes the primary conceptual artifact. Construction proceeds through four stages: (1) governance-problem identification, (2) governance-requirement and doctrinal derivation, (3) governance-requirements specification, and (4) comparative and scenario-based conceptual evaluation. Antecedent DFAS research provides conceptual input but is not treated as independent validation evidence.

In addition to the primary doctrine and its supporting governance functions, the design process generates three secondary conceptual outputs: the Governance Deployment Roadmap, the risk classification matrix in Appendix A, and the comparative governance matrices. These outputs are not independent empirical findings. The Governance Deployment Roadmap is constructed by translating the derived governance requirements into a provisional sequence of institutional onboarding, integration, and continuing assurance. The risk classification matrix is constructed by organizing the governance problems and failure conditions identified through the documentary analysis according to their implications for escalation, intervention, jurisdictional calibration, and traceability. The comparative matrices are produced through the predefined comparator-selection, dimension-coding, and classification procedures specified in the Methodology section. These secondary outputs therefore remain traceable to the same evidence-to-requirement design sequence used to construct DFAS-EconomyGov.

To establish a reproducible evidentiary basis for these stages, a targeted documentary

review was conducted on 9 September 2026. The review was designed to support conceptual derivation rather than claim exhaustive systematic coverage. It covered publications from 1992–2026, permitting earlier foundational work in regulatory and governance theory while prioritizing contemporary AI-related evidence from 2019–2026.

The search combined scholarly discovery with publisher and official institutional repositories, including sources maintained by the National Institute of Standards and Technology (NIST), Financial Stability Board (FSB), Bank for International Settlements (BIS), World Trade Organization (WTO), EUR-Lex, and International Organization for Standardization (ISO), together with academic publisher and DOI records. The search protocol comprised 28 documented search queries addressing AI governance implementation, algorithmic market integrity and collusion, financial-system AI risk, technological and third-party concentration, supply-chain resilience, digital sovereignty and jurisdiction, responsive regulation, meta-regulation, polycentric governance, and accountability.

Sources were included where they were peer-reviewed scholarly works or authoritative regulatory, institutional, or standards documents and directly informed at least one of four analytical purposes: governance-problem identification, theoretical anchoring, comparator evaluation, or scenario construction. Sources were excluded where they were non-peer-reviewed commentary for which stronger evidence was available, purely technical AI studies without a material governance dimension, duplicate versions, or materials lacking independent evidentiary relevance to the defined research problem.

The screening procedure followed the sequence relevance screening → source-type verification → domain coding → inclusion/exclusion decision → evidentiary-role coding. The audit corpus contained 25 logged candidate records, of which 22 were retained and three excluded under the predefined criteria. A single-reviewer coding procedure was used, with search queries, inclusion and exclusion decisions, exclusion reasons, domain classifications, and evidentiary roles recorded in an audit trail. Accordingly, the documentary review is reproducible and auditable but targeted rather than exhaustive, and it is not presented as a PRISMA-style systematic review or meta-analysis.

The methodology makes no claim of empirical validation, deployment, causal effectiveness, legal enforceability, or superiority over alternative governance arrangements. The Governance Deployment Roadmap and risk classification matrix are consequently treated as conceptually derived design outputs rather than validated operational instruments, and their practical effectiveness remains subject to subsequent empirical and institutional evaluation.

Analytical Scope and Unit of Governance

The analytical scope covers AI-mediated economic activity materially affecting market integrity, trade continuity, supply-chain resilience, institutional accountability, or legitimate jurisdictional interests. The unit of governance is: AI-mediated economic decision systems operating within financial markets, trade processes, and supply-chain infrastructures.

This includes algorithmic trading and pricing systems, predictive procurement platforms, AI-supported logistics and inventory systems, and related decision infrastructures. Because these systems may cross organizational and national boundaries, the analysis considers interactions among algorithmic decisions, institutional authority, regulatory requirements, technology providers, market structures, and jurisdictional conditions.

Stage 1 — Governance-Problem Identification

The documentary corpus was coded according to its substantive governance relevance rather than according to the terminology of the proposed doctrine. A governance problem was

retained where independent scholarly or institutional evidence documented a consequential condition affecting AI-mediated economic decisions, the condition was relevant to the defined unit of governance, and it could not be reduced solely to a general ethical principle.

For the purposes of this study, a governance problem was classified as recurring only where the underlying condition was supported by at least two independent sources, rather than appearing in a single publication or institutional document. Independence required that the sources represent distinct scholarly studies, institutional assessments, or authoritative instruments rather than duplicate or derivative accounts of the same evidence. This recurrence threshold was applied together with the retention criteria above and was intended to reduce dependence on isolated observations while preserving the analytical sequence from independent evidence → governance problem → governance requirement → doctrinal response.

Four governance problems met this recurrence criterion. First, algorithmic opacity and potentially collusive or destabilizing behavior create difficulty in moving from detection or explanation to an appropriate governance response (Calvano et al., 2020; Kirilenko et al., 2017; IMF, 2024). Second, asymmetric technological dependence and concentration arise where institutions depend on common models, datasets, infrastructure, or third-party providers while possessing incomplete technical control over those systems (FSB, 2024). Third, supply-chain fragility under algorithmic dependence arises when optimization-oriented recommendations become misaligned with disruption, compliance, continuity, or resilience requirements (Belhadi et al., 2023; Dey et al., 2023; Sunmola & Baryannis, 2024). Fourth, jurisdictional misalignment arises when cross-border AI-mediated decisions encounter heterogeneous or conflicting legal, regulatory, trade, and institutional requirements (Roberts, 2024; WTO, 2025). These categories constitute the evidence-derived problem structure used for subsequent doctrinal construction; they were not inferred from DFAS-EconomyGov itself.

Stage 2 — Governance-Requirement and Doctrinal Derivation

The four problems were translated into corresponding governance requirements. Algorithmic opacity and destabilizing interaction require explainability linked to escalation when material concerns remain unresolved. Technological dependence and supply-chain fragility require governed intervention authority bounded by available legal, technical, organizational, and contractual control. Jurisdictional misalignment requires jurisdiction-sensitive calibration. Because escalation, intervention, and recalibration generate consequential governance decisions, traceable accountability operates as a cross-cutting requirement.

These requirements produce the Alaali Economy Governance Doctrine (A-EGD) as the normative core of DFAS-EconomyGov. The derivation therefore follows: documented governance problems → derived governance requirements → doctrinal design. This sequencing prevents the proposed doctrine from serving as evidence for the problems it is intended to address. Antecedent DFAS research contributes conceptual input to construction but does not constitute independent validation evidence (Alaali, 2025a, 2025b, 2026).

Stage 3 — Architectural Operationalization

A-EGD is translated into four supporting governance functions: explainability escalation (A-MEEF), governed intervention authority (A-TOCC), jurisdiction-sensitive calibration (A-SCETM), and governance traceability (A-MIL). These mechanisms operationalize the doctrine rather than constitute separate theoretical contributions. Their functional relationship is: Detection/Explanation → Escalation → Authorized Containment or Review → Intervention/Reversal → Jurisdictional Calibration → Traceability and Review.

Implementation is modular because available controls differ across legal, technological, and organizational environments. Governance authority therefore does not imply direct technical control over an AI model. Where source code, model weights, training data, parameters, or other model-level controls are inaccessible, governance action may instead operate through outputs, workflows, human review, deployment controls, procurement requirements, contractual provisions, vendor escalation, or suspension.

Stage 4 — Comparative Governance Evaluation

DFAS-EconomyGov is compared with five established instruments: the OECD AI Principles, NIST AI RMF, Regulation (EU) 2024/1689, WTO trade governance, and ISO 28000:2022. These instruments are treated as functional comparators rather than equivalent regulatory regimes because their purposes, scopes, institutional mandates, and legal statuses differ.

The comparator set was selected using four predefined criteria. An instrument was included where it (1) was issued or maintained by an authoritative international, governmental, regulatory, or standards-setting body; (2) addressed at least one substantive component of the study's governance problem, including AI governance, risk management, market or trade governance, or supply-chain resilience; (3) provided sufficiently explicit provisions, principles, functions, or requirements to permit systematic assessment across the predefined governance dimensions; and (4) represented a distinct governance modality relevant to the study's cross-domain scope rather than substantially duplicating another comparator. On this basis, the OECD AI Principles represent international normative AI principles; NIST AI RMF represents organizational AI risk management; Regulation (EU) 2024/1689 represents binding risk-based AI regulation; WTO trade governance represents international trade and cross-border governance; and ISO 28000:2022 represents supply-chain security and resilience management. The comparator set is therefore purposive rather than exhaustive and is intended to provide functionally diverse reference points for conceptual evaluation.

The six governance arrangements are assessed across eight predefined dimensions: (1) operational authority, (2) economic-domain specificity, (3) explainability, (4) intervention authority, (5) jurisdictional sensitivity, (6) traceability, (7) market integrity, and (8) supply-chain resilience, producing 48 comparative judgments. The dimensions are operationalized as follows. Operational authority concerns whether an instrument provides or structures capacity for governance action. Economic-domain specificity concerns explicit application to economic, market, trade, financial, or supply-chain activity. Explainability concerns transparency, interpretability, explanation, or contestability requirements. Intervention authority concerns capacity to constrain, suspend, modify, reject, restrict, or otherwise govern consequential activity. Jurisdictional sensitivity concerns recognition of differing legal, regulatory, cross-border, or sovereign requirements. Traceability concerns documentation, attribution, logging, recordkeeping, or auditability. Market integrity concerns governance of risks affecting orderly, legitimate, competitive, or stable market activity. Supply-chain resilience concerns continuity, disruption, security, resilience, or recovery within supply-chain systems.

Each judgment uses the same three-category coding rule:

- Explicit — the function is directly and substantively addressed by the instrument.
- Partial — the function is addressed indirectly, conditionally, adjacently, or only within part of the instrument's scope.
- Not specific — the instrument does not specifically establish the assessed function within the comparison scope.

Primary regulatory, institutional, and standards documents constitute the principal evidence for comparator coding. Secondary literature is used for interpretation but does not

override the primary instrument. The coding unit is the instrument–dimension pair, and the same definitions and decision rules are applied across all six arrangements. Each comparative judgment is therefore intended to remain traceable to the relevant primary-source evidence and its coding rationale.

The comparison evaluates documented functional coverage, not empirical effectiveness, overall regulatory quality, legal strength, or institutional superiority. A designation of *Partial* or *Not specific* therefore does not imply that an instrument is deficient; it indicates only its relationship to the specific function being assessed.

Scenario and Stress Evaluation Protocol

Three illustrative conceptual scenarios evaluate whether the proposed governance functions remain coherent under materially different conditions: algorithmic collusion or destabilizing interaction, cross-border supply-chain disruption, and dependence on a third-party AI system without direct technical control. The scenarios are grounded in documented risk categories (Calvano et al., 2020; FSB, 2024; WTO, 2025) but are not case studies, simulations, deployed implementations, or empirical validation. Each scenario follows the same analytical sequence: risk detection → explanation/escalation → authority determination → feasible intervention → jurisdictional calibration → traceability/review.

The third scenario functions specifically as a failure-oriented stress test, examining whether the governance architecture remains conceptually meaningful when direct model-level intervention is unavailable and governance must instead operate through accessible organizational, contractual, workflow, deployment, or provider-level controls.

Conceptual Evaluation Criteria and Failure Conditions

The scenarios are evaluated against four predefined criteria. Conceptual coherence requires each governance mechanism to follow logically from an identified governance requirement. Functional coverage requires every derived requirement to map to at least one identifiable governance mechanism. Internal consistency requires mechanisms, authority relationships, and assumptions to remain mutually compatible. Applicability logic requires a feasible governance action to exist within the relevant institution's actual legal, technical, organizational, or contractual control.

DFAS-EconomyGov reaches a conceptual failure boundary where (1) a material governance problem lacks a corresponding mechanism, (2) mechanisms prescribe contradictory actions, (3) intervention depends on authority or technical control that the institution does not possess, or (4) substantive jurisdictional conflict is represented as resolved when the doctrine can only identify and escalate it.

These criteria evaluate conceptual structure, functional relationships, and failure boundaries, not empirical effectiveness. Validated activation thresholds, causal performance, implementation costs, comparative superiority, independent expert validation, and institutional testing remain outside the evidentiary scope of the present study.

FINDINGS AND DISCUSSION

Findings: Governance Problems and Derived Requirements

The documentary analysis identified four recurring governance problems meeting the recurrence and retention criteria specified in the Methodology section. Rather than restating those problems and their supporting evidence here, this section reports the principal finding arising from their synthesis: the problems generate a set of connected governance requirements for AI-mediated economic decision systems.

The analysis indicates that algorithmic opacity and potentially destabilizing behavior require explainability linked to escalation where material concerns remain unresolved. Technological dependence and supply-chain fragility require governed intervention authority bounded by the legal, technical, organizational, and contractual controls actually available to the institution. Cross-jurisdictional misalignment requires jurisdiction-sensitive calibration, while consequential escalation, intervention, and recalibration decisions create a cross-cutting requirement for traceable accountability.

The resulting requirements are therefore: Explainability Escalation → Governed Intervention Authority → Jurisdiction-Sensitive Calibration → Traceable Accountability. These requirements constitute the evidence-derived basis for the governance specification developed in the following sections. They represent the conceptual result of the documentary analysis rather than evidence that DFAS-EconomyGov is empirically effective or superior to alternative governance arrangements.

DFAS-EconomyGov and the Alaali Economy Governance Doctrine (A-EGD)

The Alaali Economy Governance Doctrine (A-EGD) constitutes the normative core of DFAS-EconomyGov, extending antecedent embedded-governance reasoning (Alaali, 2025b) and drawing on responsive regulation, meta-regulation, polycentric governance, and accountability (Ayres & Braithwaite, 1992; Parker, 2002; Bovens, 2007; Ostrom, 2010).

A-EGD comprises six design principles: Sovereignty First, aligning governance with legitimate jurisdictional requirements; Enforceability by Design, enabling authorized action within available legal, technical, contractual, and organizational control; Transparency and Contestability, preserving appropriate interpretability and challenge; Immutable Accountability, maintaining durable attribution and auditable governance records; Resilience to Drift, requiring reassessment as technological and operating conditions evolve; and Collaborative Stewardship, allocating responsibilities across authorized governance actors. Enforceability denotes operational governance capacity rather than legal enforceability, while immutability refers to durable record preservation rather than absolute technical immutability (Bovens, 2007; Ostrom, 2010).

These principles are design commitments derived from the identified governance requirements, not empirically validated principles. They are operationalized through A-MEEF, A-TOCC, A-SCETM, and A-MIL.

Governance Requirements Specification

A-EGD is translated into four linked governance functions: Detection and Explainability → Escalation → Governed Intervention → Jurisdictional Calibration → Traceability and Review. These functions constitute a governance requirements specification rather than a fully operational architecture. The present study identifies the conditions that should inform activation and the decision sequence through which governance concerns may progress, but it does not establish universal numerical thresholds or institution-independent intervention rules. Activation is therefore conditional on documented institutional criteria concerning materiality, applicable legal and regulatory obligations, available technical or contractual control, system characteristics, decision consequences, and the reversibility of intervention.

Under this specification, escalation or intervention should occur only where the relevant institution has established ex ante criteria, identified the responsible decision authority, documented the available response options, and specified how the resulting action will be reviewed and recorded. The precise thresholds remain institution-specific and require subsequent empirical calibration.

Alaali Market Explainability Escalation Framework (A-MEEF)

The Alaali Market Explainability Escalation Framework (A-MEEF) specifies a conditional escalation process linking deficiencies in explanation, contestability, or anomalous behavior to graduated governance responses. Level 1 applies where applicable explanation, contestability, and governance requirements are satisfied and no material unresolved concern is identified. Level 2 applies where an output is materially anomalous, contested, consequential, or only partially explainable and therefore requires documented review by the institutionally designated authority. Level 3 applies where required explanation or contestability cannot be achieved, the concern remains unresolved following review, and the case meets an institutionally predefined materiality criterion. At Level 3, the case proceeds to formal intervention assessment under A-TOCC.

Activation is therefore conditional on three elements: a documented governance concern, satisfaction of the institution's predefined materiality or escalation criterion, and an unresolved issue requiring a governance decision. A-MEEF does not prescribe a universal numerical threshold because materiality and acceptable explanation may differ across markets, institutions, systems, and regulatory environments. Institutions implementing the specification would therefore need to define and document applicable thresholds or qualitative decision criteria *ex ante* and assign responsibility for escalation decisions.

The decision procedure follows: Governance concern identified → applicable explanation or contestability requirement assessed → materiality criterion applied → documented review where required → resolution or escalation to formal intervention assessment. This structure connects explainability to governance consequence while avoiding presentation of unvalidated thresholds as established standards (Tabassi, 2023; Crisanto et al., 2024).

Alaali Trade Override Command Chain (A-TOCC)

The Alaali Trade Override Command Chain (A-TOCC) specifies the governance requirements for authorized intervention following escalation. Intervention is conditional on the existence of a material unresolved concern, legitimate institutional authority to act, and an available legal, technical, organizational, or contractual control through which the response can be implemented.

Once a case is referred from A-MEEF or otherwise reaches the institution's predefined intervention criterion, the designated authority should determine: (1) whether intervention is authorized, (2) which controls are actually available, (3) whether the proposed response is proportionate to the identified concern and potential consequences, and (4) whether the intervention can be appropriately documented, reviewed, and, where relevant, reversed. Available responses may include output rejection, use restriction, workflow suspension, human review, vendor or contractual controls and, where technically and legally feasible, system modification or recalibration.

The decision procedure follows: Formal escalation → authority verification → available-control assessment → proportionality and consequence assessment → authorized intervention or continued review → documentation and subsequent review. Where immediate material harm is plausibly imminent, temporary automated containment may be used only where such action has been authorized *ex ante* and its activation conditions, responsible authority, permissible scope, duration, and subsequent review requirements have been predefined by the implementing institution. The present study does not prescribe universal activation thresholds for such containment; their calibration remains institution- and context-dependent and requires empirical validation.

A-TOCC therefore specifies an authority-bounded intervention process rather than an autonomous override mechanism. Consequential actions remain attributable, justified, constrained

by actual institutional authority and technical capability, and subject to subsequent review, supporting accountability for both AI-mediated activity and institutional intervention ([Bovens, 2007](#); [Alaali, 2025a](#)).

Alaali Sovereign Calibration Engine for Trade & Markets (A-SCETM)

The Alaali Sovereign Calibration Engine for Trade & Markets (A-SCETM) provides a governance function for reconciling AI-mediated decisions with legitimate applicable jurisdictional requirements, including market rules, trade restrictions, sanctions, data-governance obligations, and authorized economic constraints.

A-SCETM distinguishes legal authority, technological capacity, and intervention authority. Formal jurisdiction does not establish that an institution can directly alter a third-party model or its parameters. Where direct recalibration is unavailable, governance may instead operate through inputs, outputs, workflows, deployment restrictions, procurement conditions, contractual obligations, vendor escalation, or suspension.

A-SCETM also does not determine the legitimacy of competing sovereign claims. Where requirements conflict, its function is to identify, document, and escalate the conflict for resolution through the competent legal or institutional process ([Roberts, 2024](#); [FSB, 2024](#); [WTO, 2025](#)).

Alaali Market Integrity Ledger (A-MIL)

The optional Alaali Market Integrity Ledger (A-MIL) provides the traceability function by recording material escalations, responsible authorities, interventions, calibration changes, justifications, timestamps, reviews, and outcomes. *Ledger* refers to the integrity and continuity of governance records rather than a prescribed blockchain technology.

A-MIL consequently supports accountability by connecting consequential decisions to identifiable actors, reasons, authority, and subsequent review ([Bovens, 2007](#)). Implementation can use existing institutional audit and record-management systems where these satisfy the required governance function.

Governance Deployment Roadmap

The governance requirements specification can be translated into institutional practice through three provisional phases, adapted from antecedent deployment reasoning ([Alaali, 2025a](#)). Consistent with the methodology specified in the Methodology section, the roadmap represents a conceptually derived implementation sequence rather than a validated deployment protocol.

Phase 1 — Doctrinal Onboarding identifies consequential AI-mediated decisions, responsible actors, escalation responsibilities, jurisdictional obligations, authority boundaries, technical-access constraints, documentation requirements, conflicts of interest, and emergency powers.

Phase 2 — Technical and Institutional Integration translates the relevant A-MEEF escalation requirements, A-TOCC intervention requirements, A-SCETM jurisdictional requirements, and A-MIL traceability functions into institution-specific governance arrangements. The appropriate controls may vary according to decision materiality, systemic significance, applicable authority, available technical or contractual capability, and intervention reversibility ([Tabassi, 2023](#); [Crisanto et al., 2024](#)).

Phase 3 — Continuing Assurance and Recalibration provides for periodic assessment of whether escalation processes operated as intended, interventions remained within authorized boundaries, jurisdictional adjustments remained legitimate, material actions were documented, and underlying governance assumptions remain appropriate as systems and operating conditions

change. Independent assurance or regulatory review may supplement internal controls where institutionally appropriate.

These phases specify a provisional governance deployment sequence rather than universal implementation requirements. Their practical feasibility, sequencing, institutional costs, and effectiveness remain subject to subsequent empirical and institutional validation.

Comparative Governance Analysis

The comparative analysis assesses functional coverage rather than quality, effectiveness, or superiority. Six governance arrangements—the OECD AI Principles, NIST AI RMF, EU AI Act, WTO trade governance, ISO 28000:2022, and DFAS-EconomyGov—were assessed across eight governance dimensions, producing 48 comparative judgments. The detailed provision-level evidence and coding rationale supporting these judgments are reported in Appendix A.3 – Comparative Governance Evidence Matrix.

The comparison demonstrates substantial existing governance coverage. OECD addresses broad principles of transparency, accountability, and robustness; NIST provides structured AI risk-management functions; the EU AI Act provides binding regulatory, oversight, documentation, and intervention mechanisms; WTO governance addresses trade and cross-border conditions; and ISO 28000:2022 addresses supply-chain security and resilience (OECD, 2024; Tabassi, 2023; European Parliament & Council of the European Union, 2024; WTO, 2025; ISO, 2022).

The principal difference identified is therefore configurational rather than elemental. DFAS-EconomyGov integrates explainability-linked escalation, authority-bounded intervention, jurisdiction-sensitive calibration, and traceable governance action within a single economic governance sequence. This comparison establishes conceptual positioning and functional coverage only; it does not demonstrate empirical effectiveness or superiority.

Operational Scenario and Stress Analysis

The scenarios are conceptual demonstrations, not empirical validation, and are used to test functional consistency and identify failure conditions.

Scenario 1 — Algorithmic Collusion in Commodity Markets

Consider autonomous pricing or bidding systems producing persistent supra-competitive patterns without explicit human coordination (Calvano et al., 2020). A-MEEF escalates materially anomalous or insufficiently explainable behavior; A-TOCC enables authorized containment or review; A-SCETM addresses jurisdictional constraints; and A-MIL records consequential actions. A key failure condition arises where poorly calibrated anomaly criteria disrupt legitimate market activity, supporting institution-specific rather than universal activation thresholds.

Scenario 2 — Cross-Border Supply-Chain Disruption

Consider an AI-enabled logistics platform facing a geopolitical shock affecting sanctions, border restrictions, data transfers, or critical goods (Craighead et al., 2020; WTO, 2025). A-SCETM identifies relevant jurisdictional changes, while A-MEEF, A-TOCC, and A-MIL support escalation, intervention, and traceability. Where jurisdictions impose incompatible requirements, DFAS-EconomyGov can document and escalate the conflict but cannot determine which sovereign claim prevails.

Scenario 3 — Stress Test: Third-Party Model Inaccessibility

Consider dependence on a proprietary AI service that prevents model-level access during a material disruption. A-TOCC shifts intervention to available controls, including output rejection,

human review, workflow restriction, contractual measures, provider substitution, or deployment suspension. A failure boundary occurs where neither direct technical control nor effective institutional alternatives exist. Governance authority therefore cannot substitute for absent technical or contractual capability (FSB, 2024).

Across the scenarios, conceptual coherence is supported by distinct but compatible mechanisms; functional coverage by identifiable roles for escalation, intervention, calibration, and traceability; and internal consistency by maintaining authority and technical-access boundaries across the mechanisms. Applicability logic fails where necessary authority, control, reversibility, or institutional capacity is absent. These findings establish conceptual design logic rather than practical effectiveness.

Theoretical Implications

DFAS-EconomyGov integrates established insights from responsive regulation, meta-regulation, polycentric governance, and accountability (Ayres & Braithwaite, 1992; Parker, 2002; Ostrom, 2010; Bovens, 2007). Its theoretical proposition is that AI-mediated economic governance may require explainability, escalation, intervention, jurisdictional calibration, and accountability to operate as connected functions within the decision process rather than as separate governance layers.

This proposition contributes directly to the principles-to-practice debate in AI governance. Existing scholarship identifies persistent difficulties in translating high-level AI principles into organizational and operational governance processes (Mäntymäki et al., 2022; Mittelstadt, 2019; Herzog et al., 2023). DFAS-EconomyGov addresses this debate by specifying a configurational pathway through which a governance concern can move from detection and explanation to escalation, authorized intervention, jurisdiction-sensitive calibration, and traceable review. The theoretical implication is therefore not that additional principles are required, but that the relationship among governance functions may be consequential to how principles are translated into decision-level action.

The configuration also connects two governance problems that are often treated separately: graduated intervention and distributed authority. Responsive regulation emphasizes escalation and context-sensitive intervention (Ayres & Braithwaite, 1992), whereas polycentric governance recognizes that authority may be distributed across multiple interacting decision centres (Ostrom, 2010). In AI-mediated markets and cross-border supply chains, these logics intersect because escalation does not necessarily lead to a single hierarchical authority. DFAS-EconomyGov therefore proposes that responsive intervention may need to operate within a polycentric environment in which regulatory, organizational, technological, and jurisdictional authority are distributed among different actors.

The resulting theoretical shift is from static or functionally separated governance toward continuing, authority-bounded, and configurational governance responsive to changing technological, institutional, and jurisdictional conditions. The contribution remains configurational rather than a claim that the constituent governance concepts are individually new or universally superior, and whether the proposed integration produces incremental governance value remains an empirical question.

Practical and Policy Implications

For regulators, firms, boards, risk functions, and auditors, DFAS-EconomyGov directs attention to whether consequential AI-mediated decisions have defined escalation procedures, intervention authority, technical-access boundaries, jurisdictional calibration, and traceable review (FSB, 2024).

Where DFAS-EconomyGov is applied, implementation may need to distinguish control over the model from control over outputs, workflows, deployment, procurement, contracts, and human review, particularly where third-party AI limits direct technical access. Where intervention controls are established, their scope and intensity should be calibrated conditionally according to decision materiality, applicable authority, available technical or contractual control, and institutional capability rather than assuming universal thresholds. These propositions remain subject to institutional and empirical validation.

Novelty and Contribution

The paper's central contribution is a governance doctrine that configures explainability escalation, authority-bounded intervention, jurisdiction-sensitive calibration, and traceable accountability within AI-mediated markets, trade, and supply chains.

Its novelty is configurational and bounded, rather than based on claiming that explainability, accountability, resilience, sovereignty, or oversight are individually new (Bovens, 2007; Ostrom, 2010; OECD, 2024; Tabassi, 2023). A-EGD provides the doctrinal core, with A-MEEF, A-TOCC, A-SCETM, and A-MIL specifying its supporting governance functions.

The present study establishes the configuration through doctrinal construction, documentary analysis, comparative assessment, and conceptual scenario evaluation. However, independent expert validation was not conducted, and the proposed configuration has not been empirically tested or institutionally deployed. The findings therefore support its conceptual coherence and positioning rather than its practical effectiveness or superiority. Whether the configuration improves governance outcomes remains an empirical question.

CONCLUSION

This study develops DFAS-EconomyGov as a conceptual governance doctrine for interconnected governance problems arising from AI-mediated markets, trade, and supply chains. The research question is answered through a configurational proposition: AI-mediated economic governance may benefit from connecting explainability to escalation, escalation to authority-bounded intervention, cross-border activity to jurisdiction-sensitive calibration, and consequential governance actions to traceability and review. Existing instruments already address many of these constituent functions; the contribution of DFAS-EconomyGov therefore lies in their economic-governance configuration rather than their individual novelty (OECD, 2024; Tabassi, 2023; ISO, 2022; WTO, 2025).

The study's theoretical implication is that the principles-to-practice problem in AI governance may depend not only on the adequacy of individual governance principles or controls, but also on how governance functions are connected at the decision level. In particular, DFAS-EconomyGov links the graduated-intervention logic of responsive regulation with the distributed-authority logic of polycentric governance, suggesting that escalation in AI-mediated economic systems may need to operate across multiple institutional and jurisdictional centres rather than through a single hierarchical authority. The doctrine therefore provides a configurational proposition that can be empirically examined rather than an alternative set of governance principles.

The practical implication is that regulators, firms, boards, risk functions, and auditors can evaluate AI-mediated economic governance not only by asking whether individual controls exist, but also whether there is a defined pathway connecting detection and explanation to escalation, legitimate intervention, jurisdictional calibration, documentation, and subsequent review. This distinction is particularly relevant where institutions possess authority over an economic decision but lack direct technical control over the underlying AI system.

What the study therefore enables beyond approaches that treat these functions separately is a single analytical sequence for examining the continuity of governance across an AI-mediated economic decision, while preserving distinctions among legal authority, technical capability, intervention responsibility, and jurisdictional constraints. The conceptual scenarios also establish boundaries to this proposition: poorly calibrated intervention may itself create harm, substantive jurisdictional conflicts may exceed the doctrine's resolving authority, and third-party technological dependence may prevent effective intervention.

Accordingly, the study establishes conceptual structure, functional relationships, comparative positioning, and identifiable failure conditions—not empirical effectiveness, legal enforceability, or superiority. Independent expert validation and institutional deployment were not conducted, and the incremental value of the proposed configuration remains subject to subsequent empirical testing.

LIMITATIONS & FURTHER RESEARCH

DFAS-EconomyGov is a conceptual and doctrinal construction without real-world deployment, independent expert validation, or evidence of improved governance outcomes. Its mechanisms may be constrained by legacy systems, cybersecurity, organizational capacity, latency, and the legal, technical, or contractual authority available to implementing institutions.

Third-party AI dependence may restrict intervention to outputs, workflows, human review, deployment, procurement, contractual controls, vendor escalation, or suspension rather than model modification (FSB, 2024). Similarly, A-SCETM can identify and escalate incompatible jurisdictional requirements but cannot resolve substantive conflicts of law or sovereign authority (Roberts, 2024; WTO, 2025).

Neither automated nor human intervention is assumed to be inherently superior: automated containment may generate false interventions, while human intervention may be slow, conflicted, or inadequately informed. DFAS-EconomyGov also structures accountability without determining substantive legal liability or eliminating institutional weaknesses such as regulatory capture, conflicts of interest, inadequate competence, or misconduct.

Finally, implementation costs and trade-offs—including latency, administrative burden, complexity, and possible constraints on innovation—remain untested. The governance requirements specification, deployment roadmap, and associated governance functions remain conceptually derived outputs rather than validated operational instruments. Their feasibility, calibration, effectiveness, and institutional consequences require subsequent empirical and independent evaluation.

Future research should progressively test the doctrine through independent expert validation, institutional pilots, intervention testing, cross-jurisdictional analysis, accountability and legal research, longitudinal assessment, and comparative governance testing.

Initial studies should assess the relevance, clarity, authority safeguards, and jurisdictional applicability of A-EGD and its supporting governance functions. Institutional pilots should then test implementation requirements, latency, cybersecurity, authority conflicts, and technical-access constraints. Subsequent research should compare automated, human, and hybrid intervention arrangements and empirically calibrate activation criteria rather than assuming universal thresholds.

Cross-jurisdictional research should examine A-SCETM under heterogeneous legal regimes and different levels of dependence on proprietary models, APIs, cloud infrastructure, datasets, and concentrated providers (FSB, 2024; Roberts, 2024). Accountability research should examine interactions among intervention authority, traceability, regulatory supervision, independent assurance, and liability regimes (Bovens, 2007).

Finally, longitudinal and comparative studies should determine whether integrating explainability, intervention, jurisdictional calibration, and traceability produces incremental governance value relative to existing or independently implemented controls. This provides the principal empirical test of DFAS-EconomyGov and allows its proposed configuration and supporting governance functions to be supported, modified, or rejected.

AI-Use Disclosure

Generative AI tools were used during manuscript preparation for language refinement, structural editing, and improving clarity and presentation. All conceptual development, theoretical positioning, methodological decisions, interpretation, scholarly claims, and final content were determined and reviewed by the author. The author takes full responsibility for the accuracy, integrity, and content of the manuscript.

REFERENCES

- Abbassy, S., Hameedi, M. L., & Hirawan, F. B. (2025). Examining the regional economic integration: Analysis of cross-border trade among ASEAN, China, and India. *International Journal of Management, Entrepreneurship, Social Science and Humanities*, 8(2), 230–253. <https://doi.org/10.31098/ijmesh.v8i2.3172>
- Alaali, H. M. H. (2025a). *DFAS doctrine compendium: Philosophical, strategic, and systemic frameworks for AI governance, crisis intervention, and algorithmic control*. SSRN. <https://doi.org/10.2139/ssrn.5367894>
- Alaali, H. M. H. (2025b). Governance deployment roadmap—Implementation frameworks and adoption protocols for the DFAS Governance Convergence Doctrine. *Journal of Islamic Banking, Economics and Policy*, 2(1), 43–65. <https://doi.org/10.63740/bjffnd45>
- Alaali, H. M. H. (2026). AI governance in financial systems: A PGCC and emerging markets convergence framework for accountability, sovereignty, and operational control. *Journal of Countries Studies*, 1–58. <https://doi.org/10.22059/JCOUNTST.2026.412773.1476>
- Almeida, P. G. R. de, & dos Santos Júnior, C. D. (2024). Artificial intelligence governance: Understanding how public organizations implement it. *Government Information Quarterly*, 41, Article 102003. <https://doi.org/10.1016/j.giq.2024.102003>
- Ayres, I., & Braithwaite, J. (1992). *Responsive regulation: Transcending the deregulation debate*. Oxford University Press. <https://doi.org/10.1093/oso/9780195070705.001.0001>
- Belhadi, A., Kamble, S. S., Jabbour, C. J. C., Gunasekaran, A., Ndubisi, N. O., & Venkatesh, M. (2023). Artificial intelligence techniques for enhancing supply chain resilience: A systematic literature review, holistic framework, and future research. *Computers & Industrial Engineering*, 186, Article 109714. <https://doi.org/10.1016/j.cie.2023.109714>
- 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>
- Buasan, B., Mayastinasari, V., Wahyuni, S., & Rachmawati, R. (2026). Multi-stakeholder MSME collaboration for economic resilience: A systematic literature review of Asian governance. *International Journal of Management, Entrepreneurship, Social Science and Humanities*, 10(1), 105–130. <https://doi.org/10.31098/ijmesh.v10i1.4126>
- Calvano, E., Calzolari, G., Denicolò, V., & Pastorello, S. (2020). Artificial intelligence, algorithmic pricing, and collusion. *American Economic Review*, 110(10), 3267–3297. <https://doi.org/10.1257/aer.20190623>
- Craighead, C. W., Ketchen, D. J., Jr., & Darby, J. L. (2020). Pandemics and supply chain management research: Toward a theoretical toolbox. *Decision Sciences*, 51(4), 838–866. <https://doi.org/10.1111/dec.12468>

- Crisanto, J. C., Leuterio, C. B., Prenio, J., & Yong, J. (2024). *Regulating AI in the financial sector: Recent developments and main challenges* (FSI Insights No. 63). Bank for International Settlements.
- Dey, P. K., Chowdhury, S., Abadie, A., Yaroson, E. V., & Sarkar, S. (2023). Artificial intelligence-driven supply chain resilience in Vietnamese manufacturing small- and medium-sized enterprises. *International Journal of Production Research*, 62(15), 5417–5456. <https://doi.org/10.1080/00207543.2023.2179859>
- Dong, S., Zeng, W., Aroles, J., & Tse, Y. K. (2026). When AI ethics fail and trigger negative spillovers on customer firms: Evidence from event study and fsQCA. *International Journal of Operations & Production Management*, 46(8), 1279–1302. <https://doi.org/10.1108/IJOPM-10-2025-1101>
- 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.
- Financial Stability Board. (2024). *The financial stability implications of artificial intelligence*.
- Fiss, P. C. (2007). A set-theoretic approach to organizational configurations. *Academy of Management Review*, 32(4), 1180–1198. <https://doi.org/10.5465/amr.2007.26586092>
- Hagendorff, T. (2020). The ethics of AI ethics: An evaluation of guidelines. *Minds and Machines*, 30, 99–120. <https://doi.org/10.1007/s11023-020-09517-8>
- Herzog, C., Lauber-Rönsberg, A., & Sörgel, P. (2023). Reflections on putting AI ethics into practice: How three AI ethics approaches conceptualize theory and practice. *Science and Engineering Ethics*, 29, Article 21. <https://doi.org/10.1007/s11948-023-00443-3>
- Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, 28(1), 75–105. <https://doi.org/10.2307/25148625>
- International Monetary Fund. (2024). Advances in artificial intelligence: Implications for capital market activities. In *Global financial stability report, October 2024: Steadying the course—Uncertainty, artificial intelligence, and financial stability*.
- International Organization for Standardization. (2022). *ISO 28000:2022 security and resilience—Security management systems—Requirements*.
- Kirilenko, A. A., Kyle, A. S., Samadi, M., & Tuzun, T. (2017). The Flash Crash: High-frequency trading in an electronic market. *The Journal of Finance*, 72(3), 967–998. <https://doi.org/10.1111/jofi.12498>
- Kleiner, J. (2026). Governance of AI and by AI: Feedback loops, regime variation and reflexive polycentric control. *Global Policy*, 17(3), 500–505. <https://doi.org/10.1111/1758-5899.70177>
- Li, M., & Li, T. (2022). AI automation and retailer regret in supply chains. *Production and Operations Management*, 31(1), 83–97. <https://doi.org/10.1111/poms.13498>
- MacInnis, D. J. (2011). A framework for conceptual contributions in marketing. *Journal of Marketing*, 75(4), 136–154. <https://doi.org/10.1509/jmkg.75.4.136>
- Mäntymäki, M., Minkkinen, M., Birkstedt, T., & Viljanen, M. (2022). Defining organizational AI governance. *AI and Ethics*, 2, 603–609. <https://doi.org/10.1007/s43681-022-00143-x>
- Mittelstadt, B. (2019). Principles alone cannot guarantee ethical AI. *Nature Machine Intelligence*, 1, 501–507. <https://doi.org/10.1038/s42256-019-0114-4>
- Mökander, J., Morley, J., Taddeo, M., & Floridi, L. (2021). Ethics-based auditing of automated decision-making systems: Nature, scope, and limitations. *Science and Engineering Ethics*, 27, Article 44. <https://doi.org/10.1007/s11948-021-00319-4>
- Organisation for Economic Co-operation and Development. (2024). *OECD AI principles*.
- Ostrom, E. (2010). Beyond markets and states: Polycentric governance of complex economic systems. *American Economic Review*, 100(3), 641–672.

<https://doi.org/10.1257/aer.100.3.641>

- Parker, C. (2002). *The open corporation: Effective self-regulation and democracy*. Cambridge University Press. <https://doi.org/10.1017/CBO9780511550034>
- Prem, E. (2025). A systemic perspective on bridging the principles-to-practice gap in creating ethical artificial intelligence solutions—A critique of dominant narratives and proposal for a collaborative way forward. *Journal of Responsible Innovation*. <https://doi.org/10.1080/23299460.2024.2431350>
- Raji, I. D., Smart, A., White, R. N., Mitchell, M., Gebbru, 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). Association for Computing Machinery. <https://doi.org/10.1145/3351095.3372873>
- Roberts, H. (2024). Digital sovereignty and artificial intelligence: A normative approach. *Ethics and Information Technology*, 26, Article 70. <https://doi.org/10.1007/s10676-024-09810-5>
- Singh, D., Sharma, A., Singh, R. K., & Rana, P. S. (2025). Augmenting supply chain resilience through AI and big data. *Business Process Management Journal*, 31(2), 631–657. <https://doi.org/10.1108/BPMJ-04-2024-0260>
- Sunmola, F., & Baryannis, G. (2024). Artificial intelligence opportunities for resilient supply chains. *IFAC-PapersOnLine*, 58(19), 813–818. <https://doi.org/10.1016/j.ifacol.2024.09.195>
- Tabassi, E. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)* (NIST AI 100-1). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.AI.100-1>
- Weick, K. E. (1989). Theory construction as disciplined imagination. *Academy of Management Review*, 14(4), 516–531. <https://doi.org/10.5465/amr.1989.4308376>
- World Trade Organization. (2025). *World trade report 2025: Making trade and AI work together to the benefit of all*.

Appendix A – Preliminary Risk Classification Matrix for Governance Activation

This appendix provides non-prescriptive guidance for classifying governance risk and informing the activation intensity of A-MEEF and A-TOCC. The matrix is a conceptual design instrument rather than a validated risk model, regulatory standard, or automated intervention rule. Its dimensions reflect governance concerns associated with rapid algorithmic interaction, systemic propagation, reversibility, regulatory exposure, and operational resilience identified in financial-market and supply-chain literature (Kirilenko et al., 2017; Craighead et al., 2020; FSB, 2024; IMF, 2024).

Appendix A.1 Risk Assessment Dimensions

Risk Dimension	Lower-Risk Condition	Higher-Risk Condition	Indicative Evidence Base
Event Velocity	Effects develop gradually, allowing structured review.	Effects emerge at algorithmic speed, reducing available intervention time.	Kirilenko et al. (2017); IMF (2024)
Potential Severity	Limited financial or operational consequences.	Major financial, operational, market, or systemic consequences.	IMF (2024); FSB (2024)
Propagation Risk	Effects are likely to remain localized.	Effects may propagate across markets, institutions, jurisdictions, or supply chains.	FSB (2024); Dong et al. (2026)

Reversibility	Decisions or Consequences are difficult, Tabassi (2023); consequences can be costly, or impossible to Crisanto et al. readily reversed or reverse. (2024) contained.
Legal Regulatory Exposure	/ Limited compliance or Material legal, regulatory, Roberts (2024); jurisdictional sanctions, or cross- WTO (2025) implications. jurisdictional exposure.
Systemic Materiality	Limited institutional or Potential market-wide, cross- IMF (2024); FSB network significance. border, supply-chain, or (2024) critical-infrastructure significance.

These dimensions are derived from the risk conditions identified in the documentary analysis and are conceptual assessment criteria rather than empirically validated predictors. The cited sources provide the evidentiary basis for the relevance of each dimension but do not establish the specific lower- and higher-risk classifications proposed here. Their relevance and relative importance may vary by market, institution, AI application, jurisdiction, and decision context.

Appendix A.2 – Indicative Governance Classification

Risk Level	Indicative Governance Response	Indicative Evidence Base
Low	Routine processing and monitoring; A-MEEF Level 1 may remain appropriate.	Tabassi (2023); OECD (2024)
Moderate	Enhanced scrutiny, explanation, and documentation; escalation through A-MEEF may be warranted.	Tabassi (2023); Crisanto et al. (2024)
High	Formal escalation and authorized review; A-TOCC intervention or predefined containment may be considered where institutionally authorized.	Crisanto et al. (2024); FSB (2024)
Critical	Predefined containment may be activated where legally and institutionally authorized, followed by expedited A-TOCC review, attribution, documentation, and reassessment.	FSB (2024); Crisanto et al. (2024)

The categories Low, Moderate, High, and Critical are ordinal conceptual classifications and do not represent validated quantitative thresholds. The cited sources support the underlying governance considerations concerning risk management, escalation, authority, and intervention but do not establish these four DFAS-EconomyGov classifications. Assignment should depend on the combined risk configuration rather than any single dimension. For example, moderate potential severity may justify stronger governance where propagation is rapid and consequences are difficult to reverse. Conversely, a potentially severe event with low immediacy, limited propagation, and high reversibility may permit structured review before intervention.

Activation should also remain bounded by actual institutional authority and technical control. Where an institution cannot directly modify or suspend an externally controlled AI model, feasible responses may instead include rejecting an output, escalating human review, restricting workflow use, suspending deployment, invoking contractual or vendor controls, or referring the matter to an authorized regulator or supervisory body (Crisanto et al., 2024; FSB, 2024).

Accordingly, the matrix serves as a conceptual governance activation guide rather than an automated decision rule. Institutions applying DFAS-EconomyGov would need to establish

application-specific definitions, authority boundaries, escalation procedures, evidence requirements, and containment conditions. Numerical thresholds, weighting structures, and decision rules should be established only through subsequent empirical calibration and validation.

Appendix A.3 – Comparative Governance Evidence Matrix

This appendix provides the provision-level evidentiary basis for the 48 comparative judgments reported in the Results and Discussion section. Ratings are Explicit where a function is directly addressed, Partial where coverage is indirect, conditional, or limited in scope, and Not specific where the function is not specifically established. The assessment concerns functional coverage rather than quality, effectiveness, or superiority.

Governance Dimension	OECD AI Principles	NIST AI RMF	EU AI Act	WTO Trade Governance	ISO 28000:2022	DFAS-EconomyGov
Operational authority	Partial ¹	Partial ²	Explicit ³	Partial ⁴	Partial ⁵	Explicit ⁶
Economic-domain specificity	Partial ⁷	Partial ⁸	Partial ⁹	Explicit ¹⁰	Explicit ¹¹	Explicit ¹²
AI transparency / explainability	Explicit ¹³	Explicit ¹⁴	Explicit ¹⁵	Not specific ¹⁶	Not specific ¹⁷	Explicit ¹⁸
Intervention authority	Partial ¹⁹	Partial ²⁰	Explicit ²¹	Not specific ²²	Partial ²³	Explicit ²⁴
Jurisdictional sensitivity	Partial ²⁵	Partial ²⁶	Explicit ²⁷	Explicit ²⁸	Partial ²⁹	Explicit ³⁰
Governance traceability	Partial ³¹	Explicit ³²	Explicit ³³	Partial ³⁴	Explicit ³⁵	Explicit ³⁶
Algorithmic market-integrity orientation	Partial ³⁷	Partial ³⁸	Partial ³⁹	Partial ⁴⁰	Not specific ⁴¹	Explicit ⁴²
AI-mediated supply-chain resilience	Partial ⁴³	Partial ⁴⁴	Partial ⁴⁵	Partial ⁴⁶	Partial ⁴⁷	Explicit ⁴⁸

A.3.1 Evidence Supporting the 48 Comparative Judgments

¹ OECD Principles 1.2–1.5 establish human oversight, risk management, accountability, and safeguards but do not confer regulatory authority (OECD, 2024).

² NIST AI RMF Core, particularly GOVERN and MANAGE, structures organizational governance and risk-response capacity but remains voluntary (Tabassi, 2023).

³ EU AI Act Articles 20 and 74–99 establish corrective action, market surveillance, enforcement, and penalties (European Parliament & Council of the European Union, 2024).

⁴ WTO governance structures trade rules, cooperation, transparency, dialogue, and policy coordination but does not provide organization-level AI control authority (WTO, 2025).

⁵ ISO 28000:2022 establishes organizational security-management requirements but does not itself confer public regulatory authority (ISO, 2022).

⁶ DFAS-EconomyGov specifies authority-bounded escalation and intervention through A-MEEF and A-TOCC.

⁷ OECD AI Principles apply across economic and social contexts rather than to a dedicated economic sector (OECD, 2024).

⁸ NIST AI RMF is expressly non-sector-specific and use-case agnostic (Tabassi, 2023).

⁹ The EU AI Act is horizontal regulation, although it applies to economically consequential domains, including financial services and market-facing activities (European Parliament & Council of the European Union, 2024).

¹⁰ WTO governance is explicitly concerned with international trade, trade-related policy, digital trade, and cross-border economic activity (WTO, 2025).

¹¹ ISO 28000:2022 explicitly covers security-management systems with aspects relevant to the supply chain (ISO, 2022).

¹² DFAS-EconomyGov is expressly designed for AI-mediated markets, trade, financial activity, and supply-chain infrastructures.

¹³ OECD Principle 1.3 explicitly establishes transparency and explainability, including information enabling affected parties to understand and challenge AI outputs (OECD, 2024).

¹⁴ NIST AI RMF §§3.4–3.5 and the MAP/MEASURE functions explicitly address accountability, transparency, explainability, interpretability, and documentation (Tabassi, 2023).

¹⁵ EU AI Act Articles 13–14 establish transparency, information, interpretation, and human-oversight requirements for high-risk systems (European Parliament & Council of the European Union, 2024).

¹⁶ WTO materials discuss trustworthy AI, transparency, and regulatory cooperation but do not establish a dedicated operational AI explainability requirement comparable to AI-specific governance instruments (WTO, 2025).

¹⁷ ISO 28000:2022 is a security and resilience management standard rather than an AI explainability instrument (ISO, 2022).

¹⁸ DFAS-EconomyGov makes explanation and contestability an explicit component of A-MEEF escalation.

¹⁹ OECD Principle 1.4 provides for AI systems to be overridden, repaired, or safely decommissioned where appropriate, but does not establish binding intervention authority (OECD, 2024).

²⁰ NIST AI RMF MANAGE 4.1 includes appeal, override, decommissioning, incident response, recovery, and change management, but the framework does not confer legal intervention powers (Tabassi, 2023).

²¹ EU AI Act Article 20 requires corrective actions, including bringing systems into conformity, withdrawal, disabling, or recall, supplemented by market-surveillance and enforcement powers (European Parliament & Council of the European Union, 2024).

²² WTO trade governance does not establish direct authority to suspend, modify, reject, or disable an AI system (WTO, 2025).

²³ ISO 28000:2022 requires security risk management and organizational response but is not an AI-specific intervention regime (ISO, 2022).

²⁴ A-TOCC expressly structures authorized containment, rejection, restriction, suspension, reversal, human review, and other feasible governance responses.

²⁵ OECD principles require context-sensitive conduct and alignment with applicable international law but do not create a jurisdiction-calibration mechanism (OECD, 2024).

²⁶ NIST AI RMF recognizes that risk tolerance and responses are affected by applicable laws, regulations, sector requirements, and organizational contexts, but it does not govern conflicts

among jurisdictions (Tabassi, 2023).

²⁷ EU AI Act Article 2 expressly establishes territorial and cross-border scope, including specified application to providers and deployers outside the Union (European Parliament & Council of the European Union, 2024).

²⁸ WTO governance directly addresses international trade rules, domestic-policy interaction, regulatory fragmentation, and international cooperation (WTO, 2025).

²⁹ ISO 28000:2022 provides a broadly applicable management-system structure but does not establish a dedicated mechanism for reconciling heterogeneous AI jurisdictions (ISO, 2022).

³⁰ A-SCETM explicitly separates legal authority, technical capacity, and intervention authority and calibrates governance action to applicable jurisdictional conditions.

³¹ OECD Principle 1.5 establishes accountability and lifecycle traceability, although it does not prescribe a detailed operational logging architecture (OECD, 2024).

³² NIST AI RMF GOVERN, MAP, MEASURE, and MANAGE require documentation, monitoring, tracking, reporting, and review of AI risks and responses (Tabassi, 2023).

³³ EU AI Act Articles 12 and 18–19 establish recordkeeping, technical-documentation, and logging requirements for high-risk AI systems (European Parliament & Council of the European Union, 2024).

³⁴ WTO governance uses transparency, notification, review, and institutional information mechanisms, but not a dedicated lifecycle AI audit trail (WTO, 2025).

³⁵ ISO 28000:2022 establishes documented security-management processes and auditable management-system requirements (ISO, 2022).

³⁶ A-MIL provides a dedicated record-integrity layer for detection, escalation, intervention, calibration, attribution, and subsequent review.

³⁷ OECD principles address robustness, safety, accountability, information integrity, and responsible AI conduct, which are relevant to market integrity but are not dedicated market-integrity rules (OECD, 2024).

³⁸ NIST AI RMF addresses systemic and organizational AI risks but is expressly non-sector-specific and contains no dedicated algorithmic-market-integrity regime (Tabassi, 2023).

³⁹ The EU AI Act contains market-surveillance and corrective mechanisms relevant to economically consequential AI but is not specifically an algorithmic market-integrity regime (European Parliament & Council of the European Union, 2024).

⁴⁰ WTO governance supports rules-based, transparent, and predictable international trade and addresses AI-related regulatory fragmentation, providing indirect rather than dedicated algorithmic-market-integrity coverage (WTO, 2025).

⁴¹ ISO 28000:2022 addresses security and resilience rather than algorithmic competition, trading behavior, pricing integrity, or financial-market stability (ISO, 2022).

⁴² DFAS-EconomyGov expressly addresses algorithmic interaction, potentially collusive or destabilizing behavior, escalation, and authorized market-governance response.

⁴³ OECD robustness, safety, risk-management, and stakeholder provisions can apply to AI used within supply chains, but the principles do not establish a dedicated AI supply-chain resilience regime (OECD, 2024).

⁴⁴ NIST AI RMF GOVERN 6 explicitly addresses third-party software, data, and other supply-chain issues, including contingency processes for failures in high-risk third-party AI systems, but does not constitute a dedicated supply-chain resilience framework (Tabassi, 2023).

⁴⁵ The EU AI Act addresses providers, importers, distributors, downstream actors, critical infrastructure, monitoring, and corrective action, giving partial relevance to AI-mediated supply-chain resilience without establishing a general supply-chain resilience doctrine (European Parliament & Council of the European Union, 2024).

⁴⁶ WTO materials address AI-enabled trade, supply-chain visibility, trade risks, regulatory fragmentation, and cross-border disruption conditions, but not an operational AI supply-chain resilience architecture (WTO, 2025).

⁴⁷ ISO 28000:2022 explicitly addresses security and resilience relevant to supply chains, but because it is not AI-specific its coverage of AI-mediated supply-chain resilience is coded Partial (ISO, 2022).

⁴⁸ DFAS-EconomyGov explicitly integrates AI-mediated supply-chain disruption, resilience, jurisdictional change, escalation, intervention, and traceability through A-SCETM, A-MEEF, A-TOCC, and A-MIL.

A.3.2 Comparative Interpretation

The provision-level evidence confirms substantial existing governance coverage rather than an absence of relevant mechanisms. OECD directly addresses transparency, accountability, robustness, traceability, and context-sensitive risk management; NIST operationalizes governance through Govern, Map, Measure, and Manage, including third-party and supply-chain risks; the EU AI Act provides binding coverage of intervention, jurisdiction, documentation, monitoring, and enforcement; WTO governance provides trade and cross-border orientation; and ISO 28000:2022 provides dedicated supply-chain security and resilience coverage (OECD, 2024; Tabassi, 2023; European Parliament & Council of the European Union, 2024; WTO, 2025; ISO, 2022).

The comparison therefore does not support a claim that the constituent governance functions are absent from existing instruments. Instead, coverage is less uniform at the intersection of economic-domain-specific intervention, algorithmic market integrity, jurisdiction-sensitive AI governance, and AI-mediated supply-chain resilience. DFAS-EconomyGov's distinction lies primarily in its configuration of these functions rather than their individual existence.

DFAS-EconomyGov connects explainability-linked escalation, authority-bounded intervention, jurisdiction-sensitive calibration, and traceable governance action within one economic governance sequence. Its Explicit ratings represent conceptual design coverage, not empirical effectiveness or superiority. Whether this integration improves governance outcomes requires empirical evaluation.