JOURNAL OF CULTURAL ANALYSIS AND SOCIAL CHANGE

Journal of Cultural Analysis and Social Change,
2025, 10(4), 3860-3880
ISSN: 2589-1316

Legal Gaps, Islamic Ethics, and Digital Trust: Building a Regulatory Framework for Saudi E-Commerce Under Vision 2030

Abdulrahman Aloufi[1*], Muhammad Akbar Khan[2], Bilal Hussain[3]

[1] *Dar Al-Hekma University, Saudi Arabia, Email: aaloufi@dah.edu.sa*
[2] *Dar Al-Hekma University, Saudi Arabia, Email: makbar@dah.edu.sa*
[3] *Faculty of Law, University of Sialkot, Pakistan, Email: bilal.hussain@uskt.edu.pk*

*__Corresponding Author:__ aaloufi@dah.edu.sa

Citation: Aloufi, A., Khan, M. A. & Hussain, B. (2025). Legal Gaps, Islamic Ethics, and Digital Trust: Building a Regulatory Framework for Saudi E-Commerce Under Vision 2030, *Journal of Cultural Analysis and Social Change*, 10(4), 3860-3880. https://doi.org/10.64753/jcasc.v10i4.3678

Published: December 26, 2025

ABSTRACT

Saudi Arabia's rapid e-commerce expansion under Vision 2030 has outpaced regulatory development, creating critical gaps in trusted seller verification that undermine consumer protection and Islamic commercial ethics. Despite legal frameworks including the 2019 E-Commerce Law and 2008 Anti-Commercial Fraud Law, the absence of enforceable identity verification standards, undefined platform liability, and disconnection from Islamic trade norms such as amānah (trust), tadlīs (deception), and gharar (uncertainty) threaten market integrity and sharīʿah compliance. This study argues that effective e-commerce regulation requires unified integration of legal enforcement, technological infrastructure, and Islamic ethical principles. Through hybrid doctrinal analysis combining comparative benchmarking of EU, US, and Chinese models with classical and contemporary sharīʿah scholarship, the research examines how global best practices can be adapted within Saudi Arabia's dual legal system. The study proposes a three-pillar regulatory framework: (1) legal-policy reform mandating seller verification through national digital infrastructure; (2) tiered, risk-based compliance mechanisms integrating AI-driven monitoring and blockchain verification; and (3) institutionalized Islamic ethical alignment embedding maqāṣid al-sharīʿah i.e. objectives of Islamic law into RegTech systems. This framework operationalizes ḥifẓ al-māl (wealth protection) and ʿadl (justice) through measurable regulatory functions.The proposed model positions Saudi Arabia as a pioneer in sharīʿah-compliant digital governance, bridging technological innovation with Islamic legal legitimacy to create enforceable, trust-centered e-commerce regulation aligned with Vision 2030's economic diversification objectives.

Keywords: Trusted-Seller Verification, Islamic Commercial Ethics, Sharīʿah Compliance, Saudi Legal Framework.

INTRODUCTION

The proliferation of digital commerce across Islamic-majority jurisdictions has revealed a fundamental tension between the goals of e-commerce legislation and the practical realities of market governance. This tension is particularly pronounced in Saudi Arabia, where Vision 2030 has positioned e-commerce as a cornerstone of economic diversification, yet regulatory infrastructure remains critically underdeveloped for addressing trusted seller verification. Despite the enactment of the 2019 E-Commerce Law and accompanying protection measures, the absence of enforceable identity verification standards, unclear platform liability frameworks, and a disconnect from Islamic commercial ethics have created an enforcement vacuum undermining both consumer trust and *sharīʿah* compliance.

The significance of this regulatory gap extends beyond technical compliance to encompass economic justice, digital sovereignty, and religious legitimacy. Saudi Arabia's e-commerce sector expanded by 207% between 2015 and 2020, reaching US$10.48 billion yet continued to face persistent issues with seller anonymity, fraud, and consumer protection failures. Recent scholarship has increasingly recognized that effective digital governance in Islamic contexts requires more than the transplantation of secular regulatory models; it necessitates the integration of *sharīʿah*-based ethical frameworks with contemporary enforcement mechanisms.

Contemporary academic discourse on e-commerce regulation in Islamic jurisdictions has bifurcated into two distinct streams. The first focuses on technical regulatory mechanisms through comparative legal analysis, examining digital identity systems, platform liability frameworks, and cross-border enforcement challenges. The second concentrates on Islamic commercial jurisprudence (*fiqh al-muʿāmalāt*) and its application to digital transactions, emphasizing classical prohibitions against deception (*tadlīs*), excessive uncertainty (*gharar*), and the requirement for trustworthiness (*amānah*).

A critical gap exists between these scholarly traditions. Technical regulatory studies offer sophisticated policy instruments but often lack normative grounding in Islamic legal theory. Conversely, Islamic jurisprudential scholarship provides rich ethical frameworks but remains disconnected from practical digital market governance challenges. This consequence has resulted in "regulatory incoherence" legal systems that are neither technically effective nor normatively legitimate within their Islamic context.

Recent comparative work examining Malaysia's blockchain-enabled halal verification, Indonesia's *sharīʿah*-compliant smart contracts, and the UAE's regulatory sandboxes demonstrates the feasibility of integrating Islamic principles with advanced regulatory technologies. However, these models have not been systematically adapted to Saudi Arabia's unique legal architecture combining *sharīʿah*-based governance with rapid digital transformation.

This research contributes by synthesizing these disconnected analytical streams through a hybrid regulatory approach, that treats Islamic commercial ethics as design principles enhancing digital governance effectiveness and legitimacy. By embedding *maqāṣid al-sharīʿah* objectives, particularly *ḥifẓ al-māl* (wealth protection), *rafʿ al-ḍarar* (harm prevention), and *ʿadl* (justice) into seller verification systems, this study demonstrates how Islamic legal theory can become a structural foundation for enforceable regulatory technology.

The analysis unfolds through several sections, beginning with Saudi Arabia's e-commerce landscape and digital trust dynamics, critically evaluating existing legal frameworks, exploring Islamic commercial principles, and drawing comparative insights from international and Islamic models. This culminates in a three-pillar regulatory framework comprising: (1) legal-policy reforms mandating seller verification through national digital infrastructure; (2) tiered, risk-based verification mechanisms integrating AI and blockchain technologies; and (3) institutionalized Islamic ethical alignment embedding *sharīʿah* principles into RegTech systems.

This research anticipates contributing theoretically by advancing Islamic jurisprudence-RegTech integration, methodologically by establishing a replicable framework for analyzing religious law-technology intersections, and practically by providing Saudi policymakers with a *sharīʿah*-compliant e-commerce regulation roadmap aligned with Vision 2030 objectives.

Legal and Market Background

Saudi Arabia’s transition to a digitally enabled economy is a central to Vision 2030 reform agenda. E-commerce, in particular, has emerged as a strategic priority, attracting state investment, regulatory modernization, and private sector innovation. This rapid growth has outpaced the development of cohesive legal frameworks, resulting in ongoing challenges related to consumer protection and market integrity.

To provide the necessary background for regulatory analysis, this section examines the economic significance and demographic dynamics of Saudi Arabia’s e-commerce landscape. It then explores behavioral dimensions of digital commerce, with particular focus on consumer trust and emerging legal implications such as those arising in immersive virtual environments. Together, these insights lay the foundation for a deeper investigation of regulatory gaps and Islamic ethical concerns.

Saudi E-Commerce Landscape

Saudi Arabia's e-commerce sector has witnessed rapid and remarkable expansion, positioning itself as one of the leading digital markets in the Middle East and North Africa (MENA) region. The shift aligns with Vision 2030, which targets diversification through digital innovation and private-sector growth.

E-commerce is positioned as a modernization lever to reduce oil dependence and build a globally competitive private sector. To support this strategic shift, government initiatives have targeted digital infrastructure, regulatory reform, and online retail entrepreneurship. Notably, the E-Commerce Law was enacted in 2019 as the Kingdom’s first dedicated legal framework for regulating digital commercial activity. Earlier, the Electronic Transactions System (1428 AH/2007) recognized electronic transactions and addressed authentication and evidentiary issues. Therefore, while the 2019 E-Commerce Law was the first comprehensive statute focused exclusively on e-

commerce, it was not the first statutory intervention in the broader domain of digital transactions. More recently, the 2021 Personal Data Protection Law addresses emerging data-governance and privacy challenges.

Demographically, a youthful, tech-savvy population (especially under 30) drives demand, with high digital literacy, mobile-first habits, and expectations for personalized, frictionless journeys. Weekly online shopping now reaches 52%, and digital-payment adoption exceeds 72%, signaling a break from cash-on-delivery. COD once dominated physical-goods purchases, in 2016, 70% of online goods were paid on delivery and only 24% by credit card. Policy now targets 70% cashless use by 2025, and cashless transactions rose from 18% in 2016 to 62%, propelled by Saudi Payments, fintech growth, and enabling regulation. Indicators include e-commerce digital-payment volumes above $5.5 billion in 2021, legal equivalence for e-contracts, e-signatures, and e-records. Cybersecurity baselines such as the Essential Cybersecurity Controls (2018) and a national strategy to protect transactions.

Retailers have adopted omni-channel strategies and digital marketing on Instagram, Snapchat, and WhatsApp. Government enablers, such as Mada cards, secure gateways, and e-store licenses, support trust and scale. Increasing use of AI personalization, augmented reality, and big-data analytics reflects a deliberate push toward sophisticated digital commerce.

Consumer Behavior and Trust Issues

Saudi e-commerce consumer behaviour reflects cultural values, demographics, and rapid technological change. Despite infrastructure and policy support, trust remains decisive in purchase decisions Government responses include the National Cybersecurity Authority, the PDPL, and disclosure rules for e-shops. Recommended practices such as robust security, trusted payments, and clear return policies, along with Online Dispute Resolution and clearer legal frameworks are viewed as critical for confidence and access to justice. One study found trust statistically insignificant during the pandemic, likely because regulation created a baseline presumption of reliability; foundational trust remains essential.

Trust is commonly operationalized via e-trust, e-satisfaction, and e-loyalty, which correlate with retention and allegiance. Consumers expect transparency, secure platforms, and responsive service; unclear returns or inconsistent delivery are read as trust breaches that drive abandonment or switching Counterfeits and misrepresentation further erode confidence, and weak seller-verification allows anonymous or fraudulent actors, especially in high-value categories. Gaps in KYC, ambiguous refunds, and complex complaints depress repeat purchasing.

The state has launched complementary measures: the Maarouf platform for checking registrations and public ratings, PDPL and the Anti-Commercial Fraud Law to codify trust safeguards. Yet enforcement and awareness gaps persist, and regulatory fragmentation limits impact. Digital-literacy gaps constrain protection for some groups. Underreported cyber incidents and the absence of a centralized ODR system weaken redress options.

Social commerce helps rebuild confidence: influencer endorsements, peer reviews, and real-time engagement often substitute for institutional assurances. Retailers that deliver localized Arabic content, responsive service, and transparent communication earn stronger trust and loyalty.

Legal Frameworks and Gaps

Saudi Arabia's e-commerce regime remains fragmented despite Vision 2030 gains. Laws have advanced recognition, transparency, and consumer rights, yet gaps persist in scope, enforcement, and digital-market fit. This section analyzes three pillars: the 2019 E-Commerce Law, the 2008 Anti-Commercial Fraud Law, and the Draft Consumer Protection Law. It evaluates seller accountability, dispute resolution, platform responsibility, and *Sharīʿah* alignment to frame subsequent proposals.

Analysis of the E-Commerce Law

The Saudi E-Commerce Law (ECL), enacted by Royal Decree No. M/126 on July 10, 2019, is the Kingdom's first dedicated statute for digital commercial activity within the Vision 2030 program. It comprises 26 articles covering service-provider obligations, consumer rights, advertising standards, and dispute-resolution mechanisms.

Strengths centre on transparency and accountability. Providers must disclose identity, commercial registration, location, and pricing. The law affirms consumer rights to withdrawal, redress for defects or non-delivery, and Arabic-language information, aligning with Islamic fairness and comparative consumer models. It also bans deceptive advertising and requires licenses with publicly displayed registration details.

Gaps remain present. Definitions of personal data, formal contract, and digital certificate are vague, and duties for subcontractors or standards for data retention and erasure are absent. There is no tailored ODR, pushing consumers to slow, costly litigation for low-value disputes. Consumer status as the weaker party is not explicit, and cross-border enforcement against foreign sellers is underdeveloped. Enforcement capacity is limited, with

overlapping mandates among agencies such as MCI and CITC. Systemic barriers such as limited publication of rulings, low consumer awareness, and the absence of class actions, further weaken protection.

Overall, the ECL is foundational but lacks the clarity, procedural innovation, and enforcement tools needed for a comprehensive, *sharīʿah*-aligned regime for trusted seller verification and platform accountability.

Anti-Fraud Law Assessment

The Anti-Commercial Fraud Law (2008), issued by Royal Decree No. M/19, anchors Saudi consumer protection by criminalizing counterfeits, false labelling, concealed defects, and fraudulent advertising. It reflects Islamic prohibitions on *ghish*, *tadlis*, and *gharar* . Yet it is poorly adapted to platform-based and cross-border e-commerce.

The 2009 Implementing Regulations focus on physical goods and storefront procedures, not digital fraud typologies such as fake stores, manipulated reviews, identity spoofing, or algorithmic deception. Enforcement tools, such as post-transaction inspections, seizures, and paper trails, do not match real-time, data-driven online fraud. Although instigators and participants are covered, platforms face no explicit liability for fraudulent listings or repeat offender sellers, and no mandate exists for automated fraud-detection systems.

Institutionally, oversight is fragmented. The Ministry of Commerce leads, but coordination with cybersecurity bodies, platforms, and the Consumer Protection Association is weak; reporting is not centralized; and cross-border cases face jurisdictional gaps. The law operates largely apart from the Electronic Transactions Law (2007) and the Anti-Cybercrime Law (2007), leaving transaction security, impersonation, phishing, and data falsification underregulated.

Sharīʿah concerns persist, absence of verification can enable *bayʿ ma la yamlik* and undermine requirements of ownership, clarity, and disclosure; dropshipping without ownership, undisclosed intermediaries, and unverified authenticity risk *gharar* and *ghish*.

Reform priorities: expand fraud definitions to cover digital and algorithmic manipulation; require seller identity verification, KYB compliance, and platform liability for persistent violations; mandate AI-driven red-flag systems at scale; and establish an ODR channel for fast redress.

In conclusion, the law provides an ethical baseline but remains analog, siloed, and technologically thin for digital commerce; targeted reforms are needed for a credible, *Sharīʿah*-aligned, digitally responsive verification regime.

Draft Consumer Protection Law

Saudi Arabia's 2022 Draft Consumer Protection Law seeks to unify a fragmented regime by repealing sectoral laws, notably the 2008 Anti-Commercial Fraud Law and the 2019 E-Commerce Law. Spanning 82 articles, it covers traditional and electronic B2C transactions and narrows "consumer" to natural persons acting for personal or family purposes, aligning with international practice.

For digital commerce, the draft mandates pre-contract disclosure of product characteristics, pricing, and terms; prohibits hidden fees, aggressive advertising, and manipulative in-app purchases targeting minors; and secures withdrawal rights, refunds, and protections against unfair terms. Institutionally, it introduces investigatory powers, administrative and criminal penalties, and complaint channels, and it lays initial foundations for ADR/ODR, though procedures remain unclear. It also recognizes collective consumer rights by enabling association-led group claims and reinforces privacy by banning unauthorized data use in line with national data-governance reforms.

Key gaps persist: an itemized, narrow definition of "misleading conduct"; no requirement for contract summaries or digital-receipt archiving; limited accommodations for persons with disabilities; weak cross-border protections; and no centralized, binding ODR for low-value, cross-jurisdictional disputes.

Islamic legal-ethical resonance is evident (transparency (*bayān*), harm prevention (*ḍarar*), and the prohibition of *gharar* align with *maqāṣid al-sharīʿah*, including *ḥifẓ al-māl* and justice in exchange) yet the draft omits explicit Islamic terminology and *maqāṣid* framing. Embedding *Sharīʿah*-aligned vocabulary could strengthen legitimacy within the Kingdom's dual legal system.

In summary, the 2022 Draft Consumer Protection Law is a major modernization step. Its impact will turn on executive regulations and future refinements to enforcement clarity, cross-border coverage, and Islamic normative integration.

Islamic Commercial Legal Principles

Statutory rules alone are insufficient in Saudi e-commerce. A legitimate regime must align with Islamic commercial jurisprudence. This section outlines operationally relevant principles that shape how digital transactions are structured, monitored, and regulated: *amānah* (trust), *tadlīs* and *gharar* (deception and excessive uncertainty), and *maqāṣid al-sharīʿah* (higher objectives). These principles supply both ethical constraints and design logic for systems of trust, justice, and accountability.

Amanah (Trust)

The principle of (trustworthiness) is foundational in Islamic commercial law and serves as both an ethical and legal standard that governs all transactions. It extends beyond mere honesty to encompass a comprehensive sense of responsibility, accountability, and integrity in handling wealth, fulfilling contracts, and protecting others' rights. In Islamic legal theory, is not simply a moral recommendation but a divine obligation (*taklīf*) that binds both individuals and institutions.

The Qur'anic imperative to uphold trusts and fulfil covenants is expressed in numerous verses, including the verse from *Sūrat An-Nisa*: "Indeed, Allah commands you to return trusts to their rightful owners; and when you judge between people, judge with fairness" (Qur'an 4:58), and the verse from *Sūrat Al-Aḥzāb:* "Indeed, We offered the trust to the heavens and the earth and the mountains, but they all declined to bear it, being fearful of it. But humanity assumed it, for they are truly wrongful to themselves and ignorant of the consequences" (Qur'an 33:72). These verses underscore the sacred and weighty nature of trust as a moral and legal obligation.

Prophet Muhammad ﷺ was known as *al-Amīn* (the Trustworthy) long before his prophethood, and his commercial dealings were marked by meticulous fairness, transparency, and concern for the rights of trading partners, including non-Muslims.

In *fiqh*, breaches of fiduciary duty trigger liability and censure.

Contemporary applications include *Sharīʿah* oversight, ethics audits, and governance controls; empirically, transparency, secure payments, privacy, and halal-content verification signal platform trustworthiness. While technologies like blockchain and digital identity protocols are increasingly proposed in broader e-commerce contexts, they are not directly addressed in this study.

In the context of Saudi Arabia's e-commerce landscape, the principle *amānah* supports verified sellers, truthful advertising, and robust consumer protection, functioning as a legal-ethical standard rather than a mere ideal.

Tadlīs (Deception) and (Uncertainty)

Islamic commercial law strictly prohibits deception and excessive uncertainty in transactions. These prohibitions are grounded in the Qur'an, Sunnah, and classical jurisprudential rulings and are intended to safeguard justice, transparency, and mutual satisfaction in contractual dealings.

Tadlīs covers misrepresentation and concealment of defects; the Prophet ﷺ warned, "Whoever deceives is not one of us," and jurists established khiyār al-*tadlīs* to rescind deceitful sales. *Gharar* forbids excessive ambiguity in subject matter, price, ownership, or delivery; only minor customary uncertainty (*yasīr*) is tolerated. Online environments heighten risks through intangible goods, platform intermediation, and information asymmetries, amplified by weak returns, unclear warranties, and limited redress. Compliance requires accurate listings, clear seller identity, and transparent policies; ratings, verified-seller badges, and third-party checks reduce *gharar* . Digital verification tools, such as blockchain records, smart-contract terms, and AI fraud detection, further operationalize transparency and accountability.

Maqāṣid al-Sharīʿah and Regulatory Design

Islamic commercial law is not merely a compilation of transactional rules but is deeply rooted in a teleological framework known as *maqāṣid al-sharīʿah* (the higher objectives of the Islamic law). This framework, elaborated by classical scholars such as Al-Ghazālī and al-Shāṭibī, identifies five essential objectives: the preservation of religion (*dīn*), life (*nafs*), intellect (*ʿaql*), lineage (*nasl*), and property (*māl*). These objectives provide the normative foundation upon which all legal rulings must rest, ensuring that Islamic law remains ethically coherent and socially beneficial.

In commerce, *ḥifẓ al-māl* (the preservation of wealth) mandates protection of property, prevention of unjust enrichment, and integrity in exchange; *ʿaql* and *nafs* support clarity of terms and consumer safety. Similarly, the protection of *ʿaql* prohibits exploitative schemes that obscure contract terms or manipulate cognitive biases, while *nafs* necessitates the safety and well-being of consumers, including the right to truthful information and effective remedies.

These objectives extend beyond individual contracts to encompass broader policy concerns such as market regulation, technological ethics, and institutional accountability. For instance, the principle of *maslahah* (public interest) allows jurists to formulate rulings that promote social welfare, even in the absence of explicit textual evidence. Likewise, the principle of *sadd al-dharāʾiʿ* (blocking the means to harm) empowers regulators to restrict practices that may lead to injustice or systemic risk, even if those practices are not expressly prohibited in primary sources.

Applying *maqāṣid*-based reasoning to the design of digital regulatory frameworks allows for ethical modernization of commercial law. This enables the integration of modern technologies, such as digital identity systems, AI-driven compliance tools, and blockchain verification, within a moral framework that ensures human

dignity, transparency, and trust. For example, seller verification systems serve the dual function of protecting consumer wealth (*ḥifẓ al-māl*) and preventing deceit (*tadlīs*), while also fostering justice (*ʿadl)* in market transactions.

Moreover, regulatory digital accountability must align legal form with *maqāṣid al-sharīʿah,* so contracts are not only formally valid but also advance justice, welfare, and moral clarity. Contemporary Islamic scholarship favors principled, adaptive interpretation to meet evolving economic and technological realities.

In the context of Saudi Arabia's digital transformation, embedding *maqāṣid al-sharīʿah* in regulatory design avoids copying secular templates, roots reforms in Islamic legal heritage, strengthens legitimacy and public trust, and makes e-commerce governance a vehicle for moral and economic empowerment.

Comparative Insights

While Islamic jurisprudence provides the ethical foundation for trusted seller verification in Saudi Arabia, a fully operational framework must also incorporate insights from global regulatory models. This section reviews digital identity, platform accountability, and regulatory innovation across the EU, US, China, Malaysia, the UAE, and Indonesia, extracting mechanisms transferable to a Saudi design that marries global rigor with Islamic legitimacy and Vision 2030 goals.

International Best Practices (EU, US, China)

Benchmark models clarify seller-verification levers: digital identity, platform accountability, and risk-based oversight adaptable to a *sharīʿah*-aligned Saudi regime.

European Union

The EU's Digital Services Act (DSA), enforced in 2024, introduces a tiered regulatory framework for digital platforms based on size and societal impact. Replacing the 2000 e-Commerce Directive, it mandates platform accountability, content moderation, and systemic risk management through a dual enforcement structure at both national and EU levels.

Enforcement Structure and Institutional Framework

The DSA adopts a shared enforcement structure between EU Member States and the European Commission. While national regulators oversee local platforms, the Commission supervises Very Large Online Platforms (VLOPs) and Search Engines (VLOSEs), with powers including algorithm audits, data access, and fines up to 6% of global turnover for non-compliance. Early enforcement has focused on systemic risks such as child safety and interface manipulation.

Compliance Strategies and Platform Responsibilities

The DSA transforms Trust & Safety from voluntary practice to legal obligation. Platforms must implement content moderation systems, designate compliance officers, and undergo internal audits. VLOPs are subject to annual systemic risk assessments and independent audits, focusing on harms such as misinformation, algorithmic bias, and impacts on minors. Risk mitigation and transparency are central to these strategies.

Layered Obligations and Due Diligence

Obligations scale by platform type and size. All intermediaries must publish clear terms of service, cooperate with takedown orders, and designate EU contact points. Hosting services must implement user notice-and-action systems and provide reasons for removals. Online platforms add complaint systems, access for trusted flaggers, and Know Your Business Customer (KYBC) rules to verify sellers. VLOPs must go further, maintaining ad and recommender repositories, facilitating researcher access, and disclosing algorithmic criteria.

Transparency as a Legal Principle

Transparency is central to the DSA. Platforms must publish annual reports on moderation, user appeals, and automated enforcement metrics. All content removals are documented in the EU Transparency Database.

Advertising must be clearly labeled, with details on targeting and sponsorship, and users must be informed about algorithmic recommendation criteria with the option to opt out. Additionally, vetted researchers can request access to platform data to examine systemic risks, supported by ECAT and enforced by the Commission.

Transparency and Oversight Mechanisms

VLOPs are required to log all removals, support user opt-outs from personalized feeds and respond to qualified researcher data requests. These measures are supported by standardized reporting templates and tools such as ECAT, reinforcing the DSA's emphasis on transparency and oversight.

Economic and Global Impact

The DSA harmonizes EU platform governance to balance innovation with accountability, improving legal clarity and aiding SMEs, yet drawing criticism for high compliance costs (estimated up to $50 billion for U.S. platforms) and risks of entrenching incumbents.

In conclusion, the DSA inaugurates a structured, rights-based model: layered obligations, rigorous enforcement, and radical transparency. As rollout continues, it is both an EU policy milestone and a global benchmark for governing the digital public sphere.

United States

Overview and Governance Philosophy

The U.S. adopts a market-driven hybrid of federal law, state enforcement, and platform self-governance. Major platforms deploy KYB, risk scoring, and seller monitoring, but consistency and transparency vary.

Federal Regulatory Framework

E-commerce oversight remains fragmented across statutes such as the E-Sign Act, COPPA, and ROSCA. The INFORM Consumers Act (2023) marks a turning point by mandating that platforms verify high-volume third-party sellers using bank details, tax IDs, and government-issued identification. Platforms must suspend non-compliant accounts but may exceed minimum standards voluntarily signaling a shift from reactive enforcement to preventative KYB integration.

State-Level Enforcement

States enforce their own "mini-FTC Acts", enabling tailored action against deceptive practices. Privacy-focused states like California have introduced stricter online data laws. Prior to the INFORM Act, several states advanced their own seller verification proposals, shaping a dynamic regulatory landscape that blends experimentation with layered enforcement.

Voluntary Compliance and Platform Protocols

Platforms continue to lead on KYB implementation, with some applying video verification and credential screening. However, oversight remains uneven particularly among peer-to-peer platforms. While trust badges and certification schemes are used to signal credibility, congressional hearings revealed that such tools are often misunderstood by users and provide little actual protection.

Institutionalizing KYB and Seller Identity Transparency

KYB has evolved into a central instrument for business identity transparency. Beyond the INFORM Act, Executive Order 13984 (2021) and the Corporate Transparency Act reflect a national consensus that scalable identity verification is essential to curbing fraud and anonymity risks.

China

Centralized Seller Verification and Real-Name Enforcement

China operates a centralized seller verification regime that links digital commerce to national identity infrastructure. E-commerce platforms must collect real-name authentication data, verify business credentials, and report seller information to government authorities. Platforms act as regulatory extensions by maintaining merchant records and facilitating registration for unlicensed sellers. This model enables strict oversight of tax compliance, licensing, and consumer protection.

Government Oversight and Compliance Efficiency

Through quarterly reporting requirements and broad regulatory access, China's approach enhances traceability and enforcement across digital markets. Real-name verification enables authorities to identify and sanction fraudulent sellers, while platforms bear liability for unlawful listings or repeat violations. The regime has improved market integrity and simplified due diligence, particularly for intellectual property enforcement.

Privacy Risks and Overregulation Concerns

Despite its effectiveness, China's identity-linked system raises concerns about data privacy, surveillance, and restricted anonymity. Critics argue that tools like the National Online ID platform may enable discretionary exclusion from online markets. Centralization also creates compliance burdens for small sellers, raising entry barriers and discouraging innovation. While Chinese regulators defend the system as essential for fairness and control, it exemplifies a state-heavy model that prioritizes oversight over decentralization.

Islamic Country Models (Malaysia, UAE, Indonesia)

In addition to global benchmarks, several Islamic-majority jurisdictions have undertaken meaningful steps to pair digital commerce and technological innovation with *Sharīʿah* compliance. These countries, particularly Malaysia, the United Arab Emirates (UAE), and Indonesia, offer relevant policy models that combine seller verification mechanisms, digital identity systems, and Islamic ethical oversight. Their approaches offer practical, legally grounded templates for Saudi design.

Malaysia has pioneered the integration of digital infrastructure into Islamic commercial governance. The national biometric ID system, *MyKad*, enables real-time identity verification across e-commerce and financial platforms. Notably, Malaysia has piloted blockchain-based halal supply chain systems, including seller verification protocols linked to certification authorities. These tools ensure the end-to-end traceability of goods and establish trust with consumers seeking *halāl*-compliant product. The government collaborates with religious scholars, regulatory bodies, and tech providers to ensure alignment with *sharīʿah* principles, particularly regarding *ḥifẓ al-māl* (wealth preservation) and the avoidance of *gharar*.

The United Arab Emirates (UAE) has developed a centralized Trusted KYC system that enables the digital onboarding of sellers through verified identity documents and national registries. This system is integrated into major e-commerce and fintech platforms, streamlining regulatory compliance while reducing entry barriers. The UAE also employs regulatory sandboxes, particularly under the Dubai Financial Services Authority (DFSA), which allows companies to test blockchain and AI-based verification tools under limited supervision before full deployment. This controlled environment fosters innovation while ensuring the legal oversight.

Indonesia, the world's most populous Muslim-majority nation, has embraced smart contracts and blockchain frameworks tailored for Islamic finance. These digital contracts are programmed with embedded prohibitions against *riba* (usury) and *gharar* (uncertainty), allowing sellers and platforms to automate *sharīʿah*-compliant transactions. Indonesia has also promoted Islamic e-commerce certification, which verifies both seller behavior and platform integrity through Islamic ethics review panels.

Several shared features emerge across these models.

- State-backed digital identity and KYB infrastructure.
- Regulator–scholar collaboration.
- Tech-driven trust tools (blockchain, biometrics).
- Sandboxes/pilots for controlled innovation.
- Institutionalized Islamic ethical oversight.

These approaches demonstrate the feasibility of embedding Islamic legal values into the operational core of digital commerce systems. Importantly, they also show that *Sharīʿah*-compliant systems need not resist technological modernization; instead, they can actively leverage it to institutionalize ethical business practices, reduce consumer risk, and ensure legal enforceability.

For Saudi Arabia, where Islamic law is constitutionally enshrined and Vision 2030 places a strong emphasis on digital transformation, these models offer adaptable mechanisms for integrating trust, transparency, and religious legitimacy into a future seller verification regime.

Lessons for Saudi Arabia

The comparative experiences of international and Islamic jurisdictions provide a blueprint for a Saudi seller verification framework that aligns with Vision 2030 and Islamic legal values. Rather than adopting any model wholesale, Saudi Arabia can synthesize adaptable components that reflect its regulatory priorities and *sharīʿah* commitments.

A. Tiered Obligations and Risk Governance: The EU's Digital Services Act (DSA) offers a scalable model of risk-based compliance, distinguishing duties by platform type and risk exposure. Saudi Arabia could apply a similar tiered model, imposing stricter requirements for cross-border and high-volume sellers while easing procedures for micro-enterprises advancing enforcement equity and system scalability.

B. Centralized Identity Infrastructure: China's real-name verification regime shows the power of integrating e-commerce with state-supervised identity systems. Saudi platforms such as Nafath, Absher, and the Tawakkalna API offer a foundation for unified seller registration. Mandating seller verification through these gateways linked to ZATCA and other authorities could improve compliance and reduce fraud, while allowing adaptation to local privacy standards.

C. Codifying KYB in Law: The U.S. INFORM Consumers Act (2023) embeds KYB protocols into federal law for high-volume sellers, requiring identity and financial verification. Saudi Arabia could replicate this by codifying minimum seller vetting standards, due diligence thresholds, and penalties in its Consumer Protection Law or a dedicated e-commerce statute promoting legal clarity and consistent enforcement.

D. Platform Co-Liability: Global trends affirm growing platform accountability. The EU penalizes non-compliant platforms, and China holds operators jointly liable for enabling unlicensed trade. Saudi regulators could impose co-liability on platforms that fail to enforce KYB or tolerate fraudulent conduct. This would reflect the Islamic legal concept of *daman al-mutassaib* (shared commercial liability), reinforcing ethical obligations in intermediary governance.

E. Islamic Legal Imperatives: *Sharīʿah* prohibits deception (*tadlīs*), ambiguity (*gharar*), and mandates *amānah* in trade. Classical rulings endorse consumer rescission (*khiyār al-tadlīs*) when misrepresentation affects consent. Saudi Arabia could institutionalize these through mandatory digital disclosures, rescission rights for misrepresentation, and seller conduct clauses grounded in amānah. These norms advance *ḥifẓ al-māl* (wealth protection) and *ʿadl* (justice).

F. Embedding *Sharīʿah* in Technical Systems: Islamic models show how *sharīʿah* compliance can be embedded into digital tools. Malaysia's MyKad-linked KYB and Indonesia's smart contracts coded to reject *riba* and *gharar* illustrate this integration. Saudi Arabia could form a *Sharīʿah*-tech advisory board to review algorithms, audit seller platforms, and issue e-commerce rulings, ensuring Islamic legitimacy in digital infrastructure.

G. Regulatory Sandboxes for Innovation: The UAE's sandbox approach enables controlled testing of biometric KYB, blockchain tools, and AI fraud detection. Saudi Arabia could pilot similar innovations under the Digital Government Authority or Saudi Central Bank, allowing phased integration of emerging technologies into the national verification regime.

By integrating these lessons, Saudi Arabia can construct a hybrid framework which is legally codified, technologically robust, and ethically grounded. The objective is not to choose between global or Islamic models, but to merge their most effective elements into a trust-based system rooted in local legal culture, *sharīʿah*, and Vision 2030. A layered, risk-calibrated, and faith-aligned model anchored in digital identity infrastructure and enforceable standards, will offer a scalable solution for building trust in the digital marketplace.

A summary table follows to consolidate these insights across regulatory and ethical dimensions

Table 1
Comparative Overview of Seller Verification Approaches in Leading Jurisdictions

Jurisdiction / Model	Identity Verification	Ethical Oversight	Tech Integration	Enforcement Framework
EU (DSA Model)	Mandatory KYB for high-volume traders	Content moderation, no religious/ethical mandate	Risk-based AI and data audits	Tiered obligations and fines
USA (FTC & State Law)	Platform-optional identity checks	No integrated ethical oversight	Limited (fraud pattern recognition)	Reactive enforcement via litigation
China (E-Commerce Law)	Real-name registration and licensing	Party-state values, not religious ethics	Blockchain in logistics, AI scoring	Platform liability codified
Malaysia (BNM + SC)	ID + *Sharīʿah* vetting for Islamic fintech	*Sharīʿah* boards, SC guidelines	RegTech encouraged	Licensed entities subject to revocation
UAE (ESCA + SCA)	Mandatory for licensed marketplaces	*Sharīʿah* compliance optional	Digital ID + regulatory sandbox	Coordinated oversight via MoC and regulators
Proposed Saudi Model	Nafath-linked mandatory KYB	Institutionalized Islamic ethics (, *tadlīs*, *maqāṣid*)	Blockchain + AI flagging + *Sharīʿah* smart contracts	Escalated penalties, ODR, ethical audits

Source: Author's elaboration based on regulatory analysis and proposed compliance model.

While global and Islamic jurisdictions offer valuable models, their solutions often remain fragmented, approaching e-commerce regulation through either through technical tools (blockchain, KYB, risk scoring) or through *fiqh*-based ethics. This difference of opinion limits the operational coherence and enforceability of trust mechanisms in digital marketplaces. In contrast, the framework proposed in this study seeks to integrate both by embedding *maqāṣid al-sharīʿah* into reg-tech, encoding *ḥifẓ al-māl, rafʿ al-ḍarar,* and *ʿadl* in platform protocols so Islamic ethics become the enforceable foundation of digital governance.

METHODOLOGY

This study employs a hybrid qualitative methodology designed to address both the legal-policy gaps in Saudi Arabia's e-commerce regulation and the operational integration of Islamic trade ethics. The approach combines doctrinal legal analysis, comparative benchmarking, thematic content analysis, and *sharīʿah*-based reasoning, aligning with Vision 2030's goals for digital transformation and ethical governance.

Research Design

The research is grounded in qualitative doctrinal analysis, examining the structure, coherence, and enforceability of current laws while integrating normative frameworks. Rather than relying on empirical sampling, the study synthesizes regulatory texts, peer-reviewed literature, and Islamic jurisprudence to assess both the formal and ethical adequacy of seller verification mechanisms.

Data Sources

The methodology draws from four core categories:

- **Saudi Legal and Regulatory Instruments:** Including the *Anti-Commercial Fraud Law (2008)*, *E-Commerce Law (2019)*, and the *Draft Consumer Protection Law*, supported by ministerial circulars and official guidance from bodies like the MoC and SDAIA.
- **Peer-Reviewed Literature:** Interdisciplinary sources spanning Islamic commercial law, digital governance, and RegTech, drawn from Scopus-indexed journals, academic monographs, and doctoral theses for depth and reliability.
- **Comparative Legal Models:** Benchmarking focused on the EU (DSA), US (INFORM Act), and China (E-Commerce Law), emphasizing identity verification, platform accountability, and traceability. Models were selected for their contrasting approaches and global influence, with official legal texts and policy summaries triangulated for accuracy.
- **Islamic Legal Scholarship:** Classical and contemporary *Sharīʿah* sources interpreting *Qurʾān*, *Sunnah*, and *fiqh*, especially in matters related to trade, risk, and compliance in modern digital contexts.

Supplementary insights were obtained from grey literature and government portals, used strictly for factual legal context (e.g., regulatory updates, institutional blogs), without drawing interpretive conclusions.

Analytical Framework

The research applies thematic content analysis to legal and policy texts, structured around three integrated components:

1. **Doctrinal Legal Analysis**: Evaluating the sufficiency and coherence of current and proposed laws.
2. **Comparative Benchmarking**: Extracting best practices from selected global and Islamic jurisdictions.
3. ***Sharīʿah* Reasoning**: Applying *maqāṣid-al-Sharīʿah* to assess ethical and operational alignment.

Insights were iteratively developed through prior commissioned reports by the author on Islamic fintech, e-commerce regulation, and trade ethics, and consolidated into the proposed verification framework presented.

Justification and Limitations

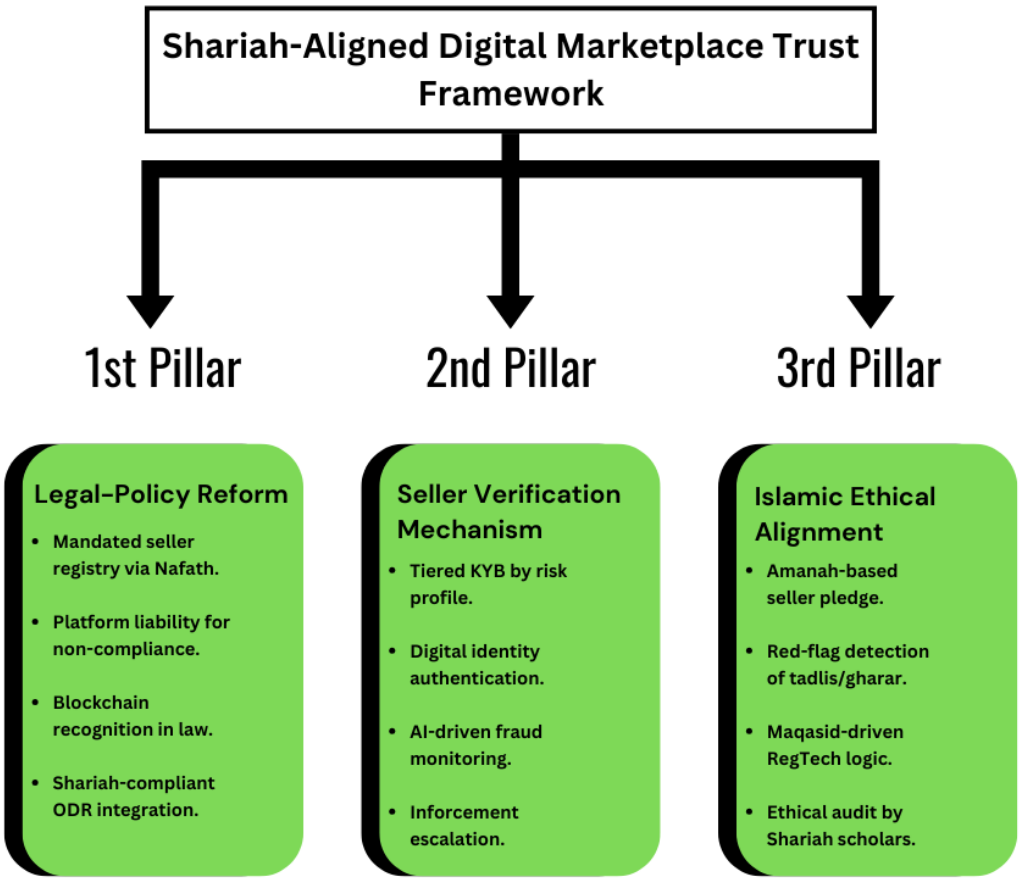
Given the interdisciplinary nature of the research, a single-method design would be inadequate. This hybrid approach enables triangulation between legal infrastructure, Islamic values, and technological feasibility.

The study does not include empirical fieldwork (e.g., interviews or surveys) nor prototype testing. These were excluded by design, as the focus is on regulatory design and jurisprudential justification. Future work may build on this to test implementation dynamics and consumer impact.

Proposed Regulatory Framework

The following presents an original regulatory framework designed to address the trust, enforcement, and ethical gaps identified in Saudi Arabia's e-commerce landscape. Grounded in both legal-policy analysis and Islamic commercial ethics. The framework is structured around three interlinked pillars: (1) legal reform to mandate seller verification and platform accountability; (2) a multi-layered verification mechanism supported by digital infrastructure and risk scoring; and (3) integration of *sharīʿah* principles such as *amānah*, *tadlīs*, and *gharar* into the operational logic of RegTech systems. Together, these pillars aim to institutionalize trust, transparency, and Islamic legitimacy across the digital marketplace.

To illustrate the structural composition of the proposed model, Figure 1 presents the three foundational pillars of the *Sharīʿah*-Aligned Digital Marketplace Trust Framework. Each pillar represents a distinct yet interconnected regulatory domain (legal-policy reform, operational enforcement, and ethical grounding) working in tandem to embed trust, accountability, and Islamic legitimacy into Saudi Arabia's evolving e-commerce ecosystem. This visual synthesis clarifies the conceptual boundaries and implementation logic of the model.



Source: Author's elaboration based on regulatory analysis and proposed compliance model.

Figure 1

sharīʿah-Aligned Digital Marketplace Trust Framework: A tripartite model comprising (1) Legal-Policy Reform, (2) Seller Verification Mechanism, and (3) Islamic Ethical Alignment.

Legal-Policy Reform

To address the structural and normative gaps identified in Saudi Arabia's current e-commerce regime, this study proposes a three-pillar regulatory framework. The first pillar focuses on targeted legal policy reforms aimed at making seller verification enforceable, technologically grounded, and aligned with Islamic legal imperatives.

A central recommendation is the mandate for a unified digital seller verification system linked to the national identity infrastructure (Nafath) and administered by the Ministry of Commerce (MoC). This would require all e-commerce sellers operating in the Kingdom, whether local or foreign, to register with a government-authorized platform that verifies their legal identity, commercial registration, and sector-specific licenses. Verified status would be a legal prerequisite for digital platform access, replacing the current informal self-disclosure practices used by platforms such as Maarouf.

In addition, the legal framework is recommended to introduce tiered platform liabilities. Marketplaces that repeatedly fail to enforce the delisting of fraudulent or noncompliant sellers should face administrative penalties and regulatory sanctions. This draws on global models, such as the European Union's Digital Services Act, which stratifies responsibilities based on platform size, risk profile, and transaction volume.

The framework also proposes that Saudi legislation explicitly recognizes blockchain-based verification mechanisms and digital compliance certificates as admissible regulatory instruments. These technologies can enhance transactional traceability, automate seller audits, and reduce compliance friction, particularly in SMEs. It is recommended that Blockchain-enabled tools are clearly defined in executive regulations and overseen by the SDAIA or the Digital Government Authority to ensure both cybersecurity integrity and regulatory interoperability.

Finally, it is recommended that the law institutionalize Online Dispute Resolution (ODR) tailored to the pace and structure of e-commerce. Unlike the current reliance on litigation and fragmented administrative channels, ODR systems can provide consumers and sellers with rapid and cost-effective remedies while enabling regulators to track patterns of noncompliance. Procedural rights, such as complaint escalation, evidence standards, and

platform response deadlines, must be codified, not merely recommended. Integrating *Sharīʿah*-compliant settlement principles (*ṣulḥ, ʿadl*) can further reinforce the system's ethical and cultural legitimacy.

Together, these reforms aim to transform Saudi Arabia's seller verification from a discretionary policy initiative into a legally enforceable, technologically integrated, and ethically grounded regulatory standard.

Seller Verification Mechanism

The second pillar of the proposed framework operationalizes the seller verification process through a multi-layered mechanism that integrates identity authentication, risk-based compliance, and AI-driven enforcement. This mechanism transforms ethical and legal norms, such as *amānah*, *tadlīs*, and *ḥifẓ al-māl*, into measurable and enforceable regulatory functions.

At the core is a mandatory registration process requiring all sellers whether individuals or businesses to authenticate their legal identity through the national digital infrastructure (Nafath) and obtain a verified seller ID linked to their commercial registration. This verified ID would serve as a prerequisite for listing products or services on any digital platform operating in Saudi Arabia. The verification process should also integrate sector-specific licensing and tax compliance records to ensure holistic diligence.

To ensure proportionality and scalability, the framework adopts a tiered, risk-based compliance model. Sellers are stratified into categories based on their transaction volume, product type (e.g., high-risk sectors such as cosmetics or health), and complaint history. Higher-tier sellers would be subject to enhanced verification protocols, including periodic reauthentication, audit trails, and public trust ratings. Lower-risk sellers, such as micro-enterprises or individual artisans, would face simplified procedures, thereby reducing entry barriers while maintaining baseline accountability. The table below outlines the proposed tier structure, compliance criteria, and corresponding verification requirements.

Table 2
Tiered Compliance Standards for Seller Verification Based on Risk and Scale

Tier	Criteria	Requirements
Tier 1	SMEs with <$100K annual sales	Basic ID + license verification
Tier 2	Mid-market ($100K–$1M)	Full KYC, refund policy transparency, data protection compliance
Tire 3	Large enterprises & high-risk sectors	Independent audits, ODR interface integration, product traceability logs

Source: Author's elaboration based on regulatory analysis and proposed compliance model.

Sellers would move between tiers based on transaction volume, sector sensitivity (e.g., health, cosmetics, food), and prior violations. Upgrades or downgrades are reviewed periodically by a supervisory authority.

AI technologies play a crucial role in monitoring seller behavior and platform compliance. Algorithms can flag anomalies in pricing patterns, detect duplicate listings across platforms, and identify inconsistencies between advertised and delivered products. These tools support the early detection of deceptive practices (*tadlīs*) and mitigate uncertainty (*gharar)* by reducing the information asymmetry. Platforms would be required to integrate such monitoring tools and report high-risk sellers to regulatory authorities through automated dashboards.

The mechanism also introduces a graduated enforcement system. First-time violations would trigger platform-level warnings and correction windows. Repeat offences would escalate to temporary suspension, blacklisting, or permanent de-verification of the account. De-verified sellers would be barred from listing on any platform governed by the Saudi e-commerce ecosystem. These enforcement actions must be transparent, appealable, and consistent across platforms to maintain legal integrity and fairness in the market.

Together, these measures form a cohesive seller verification architecture that is technologically robust, ethically grounded, and scalable. By embedding both sharīʿah principles and RegTech logic, the mechanism ensures that trust in digital commerce is not merely presumed but institutionally secured.

Islamic Ethical Alignment

The third pillar of the proposed framework embeds Islamic legal and ethical principles directly into the regulatory architecture of the seller verification process. While legal enforcement and technological infrastructure are necessary, they are insufficient unless grounded in a normative system that reflects the Kingdom's foundational commitment to *Sharīʿah*. This pillar ensures that regulatory design does not merely comply with secular benchmarks but aligns substantively with Islamic commercial jurisprudence and the *maqāṣid al-sharīʿah*.

Central to this alignment is the operationalization of *amānah* as a legally recognized seller's obligation. Verified sellers would be required to commit to an ethical pledge affirming their adherence to transparency (*bayān*), product

authenticity, and fair dealing, which are principles derived from Qur'anic imperatives and prophetic commercial ethics. This pledge would not be symbolic; it would carry legal weight and serve as a basis for both regulatory and reputational consequences in the event of *tadlīs* or *gharar* -inducing behavior in the future.

To reinforce this ethical layer, platforms must implement algorithmic integrity tools that reflect *Sharīʿah*-based risk factors. For example, repeated cases of deceptive advertising, inaccurate product labelling, or abrupt changes in seller location may trigger a review for *khiyār al-ghabn* or *khiyār al-tadlīs* breaches. These technical alerts would feed into a national ethics dashboard managed by a regulatory unit in coordination with the Council of Senior Scholars or designated *sharīʿah* boards.

The framework also proposes that certain platform design elements encode these values. Features such as sharīʿah-compliant return policies, transparent pricing structures, and pre-sale disclosures reflect the obligation to avoid *gharar* and ensure contract clarity. Where feasible, platforms may use smart contracts that auto-enforce ethical conditions, such as refund triggers for the non-disclosure of product defects or delayed delivery. These tools transform moral principles into an enforceable transaction logic.

Importantly, the institutionalization of ethical oversight is essential in this context. A specialized regulatory body or consultative council need to be empowered to conduct Islamic compliance audits of platforms, resolve doctrinal disputes in digital trade, and provide ethical guidance for emerging technologies. This structure ensures that the interpretation and application of Islamic norms are not left to discretionary or inconsistent platform policies but are grounded in qualified legal authority.

Finally, the ethical pillar is to be grounded in the objectives of *Sharīʿah* (*maqāṣid al-sharīʿah*), not merely as an interpretive framework but as a foundational design logic. Protecting wealth (*ḥifẓ al-māl*), minimizing harm (*la ḍarar*), and promoting justice (*ʿadl*) are not abstract ideals; they constitute enforceable aims. When embedded into verification systems, scoring models, and dispute resolution pathways, these principles form the backbone of a regulatory ecosystem that is both technologically advanced and spiritually as well as legally coherent.

Together, these three pillars constitute the core of the proposed regulatory framework. They define not only the normative logic of a *Sharīʿah*-compliant digital marketplace but also the structural architecture for enforceable and trustworthy e-commerce governance. In the following section, the framework's operationalization is detailed through four complementary implementation domains: institutional coordination, technology infrastructure, public capacity building, and strategic mitigation. These domains ensure the framework's practical viability and continuous adaptability to market realities.

Implementation and Monitoring

The effectiveness of the proposed regulatory framework depends not only on its legal and ethical design, but also on a coordinated and accountable implementation strategy. This section outlines the institutional, technical, and social dimensions necessary to ensure that seller verification becomes an operational reality, rather than a policy aspiration. It also proposes measurable indicators for evaluating progress and a cyclical mechanism for regulatory review.

To translate the proposed framework into actionable policy, a four-pillar implementation architecture is introduced. These pillars (Institutional Coordination, Technology Infrastructure, Public Capacity Building, and Strategic Mitigations) form the operational backbone of the system. Each identifies the entities, tools, and mechanisms required to turn legal mandates and ethical commitments into tangible outcomes. Figure 2 offers a visual overview of this structure, clarifying the distribution of responsibilities and the interdependence between regulatory, technical, and social domains.

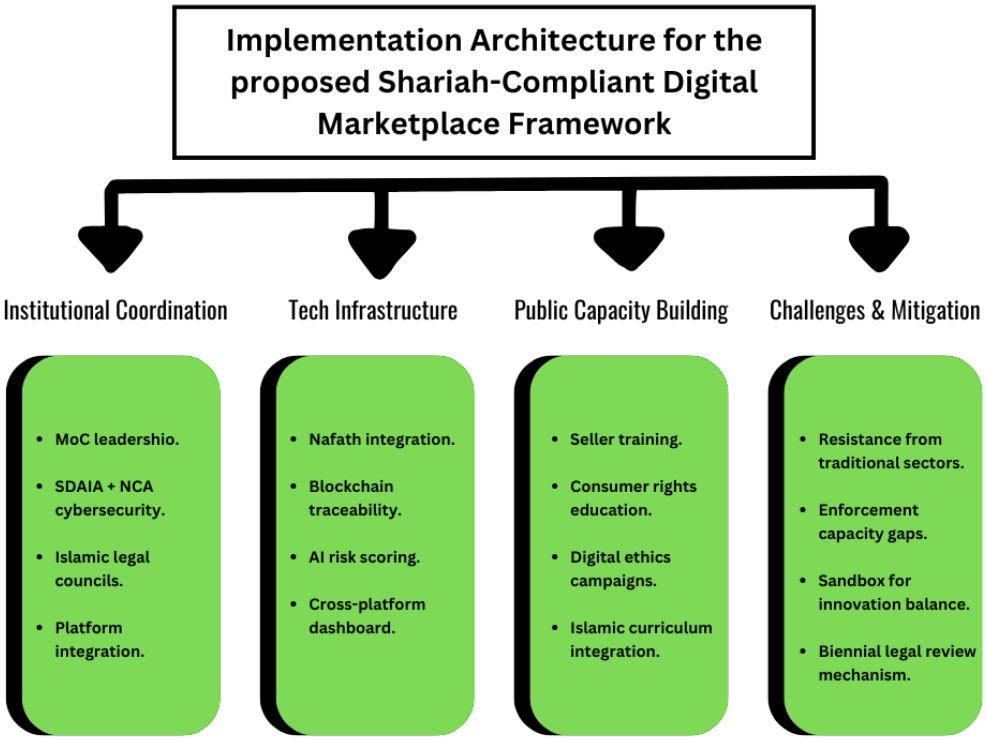


Figure 2
Implementation Architecture for Sharīʿah-Compliant Digital Marketplace Governance.
Source: Author's elaboration based on regulatory analysis and proposed compliance model.

Institutional Coordination

The successful enforcement of the seller verification framework requires collaboration among multiple regulatory bodies:

- **Lead authority:** Ministry of Commerce (registration enforcement, platform oversight, sanctions).
- **Data, AI, cybersecurity:** SDAIA and the National Cybersecurity Authority (data integrity, AI risk-scoring protocols, ethical use of blockchain tools).
- ***Sharīʿah* governance:** Council of Senior Scholars or platform *Sharīʿah* boards (ethics review of automated decisions, smart-contract design).
- **Platforms:** Local and international services licensed and bound to reporting obligations.

Technology Infrastructure

Robust infrastructure is a prerequisite for scalable seller verification.

- **Identity/KYB:** Expand Nafath with KYB modules and third-party APIs; real-time checks tied to commercial registration and sector licenses.
- **Traceability:** Blockchain ledgers for seller status, licensing, and ethical pledges.
- **Supervision:** AI risk monitoring to flag anomalies (quality drops, repeat complaints, metadata signals); regulator and platform dashboards for proactive alerts and reactive enforcement.

Public Awareness and Capacity Building

A trust-centered digital marketplace cannot be built through regulation alone; social acceptance and ethical literacy are equally important factors. Regulators should launch targeted awareness campaigns to explain the rationale, benefits, and obligations of the seller verification system.

This includes:

- **Sellers:** Training via chambers of commerce and fintech partners for onboarding and compliance.
- **Consumers:** Guidance to verify sellers, submit ethics complaints, and recognize *tadlīs*/*gharar* indicators.
- **Ethics:** Campaigns through mosques, universities, and digital influencers on *amānah* and responsible online trade.

KPIs and Legal Review Mechanism

To ensure transparency and accountability, regulators should adopt a Key Performance Indicator (KPI) dashboard to monitor the framework's operational effectiveness. The suggested indicators include:

- Percentage of verified sellers on licensed platforms
- Rate of consumer complaints resolved through ODR or regulatory channels
- Platform compliance rate with reporting and delisting obligations
- Public trust metrics, such as consumer satisfaction and platform ratings

Additionally, the entire regulatory framework should be subject to a biennial legal review to assess its relevance, enforceability, and ethical adequacy. This review process should be conducted by a joint task force composed of MoC, SDAIA, Islamic legal scholars and technology experts. These recommendations may then be incorporated into legislative amendments, technical updates, or public engagement strategies.

Implementation Challenges and Strategic Mitigations

Although the proposed framework is structurally and normatively sound, its implementation may encounter practical and institutional obstacles that require early recognition and mitigation. These challenges are not unique to Saudi Arabia but are particularly prominent in legal systems that are undergoing simultaneous digital and ethical transformations. Challenges include:

- **Incumbent resistance (informal/semi-regulated actors):** Phase-in timelines, grace periods, technical support, incentives; public–private partnerships for sector-specific guidance.
- **Technical complexity (AI, blockchain, cross-platform dashboards):** Leverage SDAIA and the Digital Government Authority; use pilots/sandboxes before scale-up; enforce interoperability and cybersecurity baselines.
- **Innovation vs oversight:** Avoid over- or under-regulation by using the biennial review as a feedback loop aligned with market realities, tech change, and evolving Islamic jurisprudence.

By anticipating these implementation challenges and embedding strategic flexibility, the framework can remain enforceable, non-rigid, and legitimate over time.

CONCLUSION

This study explored the legal and ethical foundations of seller verification in Saudi Arabia's e-commerce sector, revealing several critical gaps across existing statutes, enforcement mechanisms, and alignment with Islamic commercial jurisprudence. Although the E-Commerce Law and associated regulations reference consumer protection, they lack binding structures for identity verification, platform liability, and ethical compliance. Moreover, foundational Islamic trade principles (such as *amānah*, *tadlīs*, and *gharar*) remain largely unimplemented at the institutional level, diminishing their practical enforceability.

To address these challenges, the study proposed a tripartite regulatory framework built on:

1. Legal-policy reform.
2. A tiered and risk-based seller verification mechanism.
3. Islamic ethical alignment grounded in *maqāṣid al-sharīʿah*.

This framework leverages national digital infrastructure (e.g., Nafath), emerging technologies (e.g., blockchain, AI), and structured regulatory oversight to embed trust, transparency, and moral legitimacy into Saudi Arabia's digital marketplaces.

By aligning technology governance with Islamic ethics, the model directly supports Saudi Arabia's Vision 2030 objectives related to legal reform, digital innovation, and Islamic economic leadership. The proposed approach positions the Kingdom as both a regional pioneer and a potential global reference point for *Sharīʿah*-compliant digital regulation and ethical RegTech.

While this research is primarily doctrinal and conceptual, it opens several avenues for future empirical inquiry. These include:

- Evaluating the real-world impact of seller verification systems on consumer trust.
- Comparative case studies involving Malaysia, Indonesia, and the UAE.
- Further exploration of *Sharīʿah*-RegTech applications in areas such as Islamic fintech, smart contracts, and cross-border dispute resolution.

The author gratefully acknowledges the academic institutions, regulatory documents, and prior scholarly work that supported this research. Scholarly engagement is warmly welcomed to further develop and operationalize the framework presented herein.

REFERENCES

A. El-Gamal, Mahmoud. 'An Economic Explication of the Prohibition of Gharar in Classical Islamic Jurisprudence'. Islamic Economic Studies 08–2 (2001): 29–58. https://ideas.repec.org//a/ris/isecst/0142.html.

Abdullah, Muhamad Mu'izz, Abdul Bari Awang, and Nasrul Hisyam Nor Muhamad. 'THE ANALYSIS OF TRUST INSTRUMENTS IN MALAYSIA AS ISLAMIC ESTATE PLANNING: THE CHALLENGES AND EFFECTS'. UUM Journal of Legal Studies 13, no. No.1 (2022): 107–29. https://doi.org/10.32890/uumjls2022.13.1.5.

Adam Husik and John ReVeal. 'New FTC Guidance: The INFORM Consumers Act's Impact on Online Marketplaces' Third-Party Sellers'. Legal Blog. FinTech and Blockchain Law Watch (FinTechLawBlog), FinTechLawBlog / Sheppard Mullin Richter & Hampton LLP, 2023. https://www.fintechlawblog.com/2023/09/01/new-ftc-guidance-the-inform-consumers-acts-impact-on-online-marketplaces-third-party-sellers/.

Al Hamli, Sarah S., and Abu Elnasr E. Sobaih. 'Factors Influencing Consumer Behavior towards Online Shopping in Saudi Arabia Amid COVID-19: Implications for E-Businesses Post Pandemic'. Journal of Risk and Financial Management 16, no. 1 (2023): 1. https://doi.org/10.3390/jrfm16010036.

Alaabed, Alaa, Hossein Askari, Zamir Iqbal, and Adam Ng. 'Benchmarking Objectives of Shari'ah (Islamic Law): Index and Its Performance in Select OIC Countries'. International Journal of Pluralism and Economics Education 7, no. 3 (2016): 218. https://doi.org/10.1504/IJPEE.2016.079685.

Alabdulqader, Latifah Abdulmohshen. 'Contractual Justice under English and Shariah Law of Contract: The Case of Consumer Protection'. Thesis, Brunel University London, 2018. http://bura.brunel.ac.uk/handle/2438/15941.

Alangari, Abdalrahman. 'A Proposal for Omnibus Legal Reform of Saudi Construction Practices to Meet Economic Development Goals in Saudi Arabia: An Initiative for Legislative Reform towards Effective and Codified Judicial Remedies, Compatible with Sharia Law and Aligned with Saud'. Doctor of Juridical Science (S.J.D.) Dissertation, American University Washington College of Law, 2021. https://digitalcommons.wcl.american.edu/stu_sjd_abstracts/15.

Alatawi, Omar D. 'The Saudi Arabian Legal System's Approach to White-Collar Crimes: Challenges and Potential Reforms'. Cogent Social Sciences 10, no. 1 (2024): 2413622. https://doi.org/10.1080/23311886.2024.2413622.

Albar, Kholid, Achmad Abubakar, and Aisyah Arsyad. 'Islamic Business Ethics in Online Commerce: A Perspective from Maqashid Shariah by Imam Haramain'. JURNAL ISLAM NUSANTARA 7, no. 2 (2023): 2. https://doi.org/10.33852/jurnalnu.v7i2.501.

Albous, Mohammad Rashed, Odeh Rashed Al-Jayyousi, and Melodena Stephens. 'AI Governance in the GCC States: A Comparative Analysis of National AI Strategies'. Journal of Artificial Intelligence Research 82 (2025): 2389–422. https://doi.org/10.1613/jair.1.17619.

Albshaier, Latifa, Seetah Almarri, and M. M. Hafizur Rahman. 'A Review of Blockchain's Role in E-Commerce Transactions: Open Challenges, and Future Research Directions'. Computers 13, no. 1 (2024): 1. https://doi.org/10.3390/computers13010027.

Al-Daboubi, Derar, and Jalal Alqhaiwi. 'LEGAL AND REGULATORY FRAMEWORK FOR MONITORING ONLINE STORES'. UUM Journal of Legal Studies 13, no. 1 (2022): 1. https://doi.org/10.32890/uumjls2022.13.1.8.

Aldmour, Renad. 'Regulations and Legal Implications of Contracts through Instant Messaging Platforms in Saudi Arabia'. Pakistan Journal of Life and Social Sciences (PJLSS) 22, no. 2 (2024). https://doi.org/10.57239/PJLSS-2024-22.2.00927.

Aleid, Mohammed S. 'A Critical Analysis of Investor Protection under Saudi Stock Market Regulations'. Phd, University of Essex, 2018. https://doi.org/10/1/phd%252520thesis.pdf.

Algarni, Faris M. 'The Impact of the Saudi New E-Commerce Law on Protecting E-Commerce Investments in Saudi Arabia'. TIIKM (The International Institute of Knowledge Management), 2 October 2020, 29–38. https://doi.org/10.17501/27141888.2020.1104.

Alhejaili, Mohammad Omar Mohammad. 'Securing the Kingdom's e-Commerce Frontier: Evaluation of Saudi Arabia's Cybersecurity Legal Frameworks'. Journal of Governance and Regulation 13, nos 2, special issue (2024): 275–86. https://doi.org/10.22495/jgrv13i2siart4.

Alias, Muhammad Nazir, Muhammad Najib Abdullah, Mohd Sham Kamis, Akhmad Jazuli Afandi, and Nursyahidah Alias. 'SCIENTIFIC APPROACH AS THE BASIS FOR THE FORMATION OF MAQĀṢID AL-SHARĪ'AH CONCEPT AND PRINCIPLES: A COMPARATIVE STUDY'. Malaysian Journal of Syariah and Law 12, no. 2 (2024): 2. https://doi.org/10.33102/mjsl.vol12no2.568.

Aljaber, Abdullah. 'E-Learning Policy in Saudi Arabia: Challenges and Successes'. Research in Comparative and International Education 13, no. 1 (2018): 176–94. https://doi.org/10.1177/1745499918764147.

Alkhieli, Abdulrahman. 'Corporate Governance Reform in Saudi Arabia: A Modelling Approach'. In Institute of Advanced Legal Studies. Doctoral, University of London, 2018. https://sas-space.sas.ac.uk/9511/.

Al-Maliki, Saeed Q. Al-Khalidi. 'Increasing Non-Oil Revenue Potentiality through Digital Commerce: The Case Study in KSA'. Journal of Money and Business 1, no. 2 (2021): 65–83. world. https://doi.org/10.1108/JMB-07-2021-0022.

Almalki, Adnan. 'Legal Protection for the Consumer in E-Commerce According to Saudi Law (A Descriptive, Analytical, and Comparative Study with the Laws of the United States of America)'. Beijing Law Review 12, no. 4 (2021): 4. https://doi.org/10.4236/blr.2021.124058.

Al-mani, Khulood. 'The Impact of E-Commerce on the Development of Entrepreneurship in Saudi Arabia'. Journal of International Technology and Information Management 28, no. 4 (2020): 28–62. https://doi.org/10.58729/1941-6679.1424.

Almansoori, Saood Obaid Musabih. 'Conflict of Laws in E-Commerce in the UAE and the Prospect for Harmonization among Gulf Cooperation Council Member States'. Doctoral thesis (PhD in Law), University of Essex, School of Law, 2018.

Almebrad, Abdulaziz. 'The Sufficiency of Information Privacy Protection in Saudi Arabia'. Doctor of Juridical Science (S.J.D.), Indiana University Maurer School of Law, 2018. https://www.repository.law.indiana.edu/etd/56.

Almughyirah, Muflih. 'Rethinking the Civil Protection of Patients from Misleading Pharmaceutical Marketing Under Saudi Law'. Doctor of Juridical Science (SJD), Maurer School of Law - Indiana University, 2023. https://www.repository.law.indiana.edu/etd/119.

Almuqati, Mohammed Marzouq. 'The Impact and Challenges of Basel III Implementation in Saudi Arabia'. Doctor of Philosophy (PhD), Brunel University London, 2018. http://bura.brunel.ac.uk/handle/2438/17040.

Almutairi, Ahlam Sultan. 'Consumer Behavior and E-Commerce Adoption in the Food Industry in Saudi Arabia'. Arab Journal for Scientific Publishing 7, no. 74 (2024): 1–22. https://doi.org/10.36571/ajsp741.

Alotaibi, Ibrahim M. 'The Role of Competition Law in the Telecommunications Sector in Saudia Arabia'. Doctor of Philosophy (PhD), Brunel University London, 2019. http://bura.brunel.ac.uk/handle/2438/18916.

Aloufi, Abdulrahman. 'THE NEED TO ENHANCE ONLINE CONSUMER PROTECTION UNDER EXISTING SAUDI ARABAIN E-COMMERCE LAWS'. Doctor of Philosophy (PhD), Curtin University, School of Business and Law, 2023.

Alqahtani, Yahya Ali M. 'M-Commerce in Saudi Arabia Perspectives of Consumers and Vendors Following Vision 2030'. Thesis, University of Sussex, 2023. https://sussex.figshare.com/articles/thesis/M-commerce_in_Saudi_Arabia_perspectives_of_consumers_and_vendors_following_Vision_2030/24260641/1.

Alshahrani, Shaya. 'The Consumer Protection Bill 2022: A Quantum Leap of Consumer Policy in Saudi Arabia'. Manchester Journal of Transnational Islamic Law & Practice 19, no. 3 (2023): 277–84. https://heinonline.org/HOL/LandingPage?handle=hein.journals/jispil19&div=52&id=&page=.

Alshahrani, Shaya. 'The Legal Protection of Unfair Commercial Practices - An Analytical Study on the Anti-Commercial Fraud Law'. Jazan University Journal of Human Sciences 12, no. 2 (2024). https://doi.org/10.37575/h/edu/22002.

Alshalan, Abdulmajeed. 'Corrupt Practices in Saudi Arabia: An Analysis of the Legal Provisions and the Influence of Social Factors'. Indiana University Maurer School of Law, 2017. https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=1044&context=etd.

Al-Shamrani, Ahmed Ali Hazaa. 'Legal Frameworks for Consumer Protection in E-Commerce Contracts and Their Development in Saudi Arabia: An Analytical Comparative Study with the American System'. Majmaah Journal of Sharia and Law Sector 16 (المجلة الأكاديمية لقطاع الشريعة والقانون), no. 16 (2024). https://doi.org/10.21608/jssl.2024.320354.1094.

Alshathri, Saud Abdullah. 'Online Dispute Resolution as a Mechanism to Enhance Consumer Trust in E-Commerce: How Can Saudi Arabian Law Be Improved?' Doctor of Philosophy in Law, Newcastle University, 2022. https://theses.ncl.ac.uk/jspui/bitstream/10443/5762/1/Alshathri%20S%202022.pdf.

Alsolami, Alhanouf A. 'A Comparative Study of Consumer Arbitration and Class Action's Mechanism'. Doctoral Dissertation (S.J.D.), University of California - School of Law, 2019. https://escholarship.org/content/qt2653s8zm/qt2653s8zm.pdf.

Anti-Commercial Fraud Law 2008, Pub. L. No. 2008, M/19 Royal Decree. Promulgated by Royal Decree No. M/19 dated 23/4/1429H (29 April 2008).

Anti-Cyber Crime Law 2007, M'17 Royal Decree § Government and Politics (2007). https://saudipedia.com/en/article/2926/government-and-politics/systems/anti-cyber-crime-law-in-saudi-

arabia. Issued on 27 March 2007 by Royal Decree No. M/17.

Awwad, Ahmed, and Amal Abdelsattar. 'Digital Evidence in Forensic Accounting- A Study in Saudi Legislation'. Cogent Social Sciences 11, no. 1 (2025): 2522958. https://doi.org/10.1080/23311886.2025.2522958.

Bendary, Mohamed G., and Jegatheesan Rajadurai. 'Emerging Technologies and Public Innovation in the Saudi Public Sector: An Analysis of Adoption and Challenges Amidst Vision 2030'. Innovation Journal 29, no. 1 (2024). https://openurl.ebsco.com/contentitem/gcd:176232637?sid=ebsco:plink:crawler&id=ebsco:gcd:176232637.

Berger, Ilana, Tim Torres, and Ariella Rothschild. 'The Digital Services Act (DSA): 2024 Compliance Essentials'. Corporate blog (by a private company). ActiveFence, 9 May 2024. https://www.activefence.com/blog/digital-services-act/.

Boscheck, Ralf. 'The EU's Digital Markets Act: Regulatory Reform, Relapse or Reversal?' Intereconomics 59, no. 3 (2024): 154–59. https://doi.org/10.2478/ie-2024-0032.

Candrawati, Iin, and Shofa Robbani. 'UNDERSTANDING THE 7 KEY PROHIBITIONS IN ISLAMIC TRADE PRACTICES'. Profit : Jurnal Kajian Ekonomi Dan Perbankan Syariah 9, no. 1 (2025): 1. https://doi.org/10.33650/profit.v9i1.10642.

Channak, Zaki Mahmed, Abdulkader Alkhateeb, Elham Saleh, Hanadi Aldeeb, and Sayed Alsharif. 'Business Ethics in E-Commerce - Legal Challenges and Opportunities'. Access to Justice in Eastern Europe 2023 (2023): 1–16. https://doi.org/10.33327/ajee-18-6s007.

Charlie Osborne. 'China Introduces National Cyber ID Amid Privacy Concerns'. Cybersecurity news and analysis. Dark Reading, 2025. https://www.darkreading.com/cyber-risk/china-introduces-national-cyber-id-privacy-concerns.

Chen, Dongmei, and Wenke Han. Deepening Cooperation Between Saudi Arabia and China. Discussion Paper (KAPSARC Discussion Paper No. dp53). Riyadh, Saudi Arabia, 2019. https://www.kapsarc.org/wp-content/uploads/2019/03/Deepening-Cooperation-Between-Saudi-Arabia-and-China.pdf.

' China's New E-Commerce Law'. 2019. https://www.worldtrademarkreview.com/global-guide/anti-counterfeiting-and-online-brand-enforcement/2019-obe/article/chinas-new-e-commerce-law.

Cofer, Jack A. 'The Grey Market's Ability to Be Black and White: Regulating for Fraud in Online Marketplaces Beyond the INFORM Consumers Act'. Georgia Law Review 59, no. 2 (2025). https://georgialawreview.org/wp-content/uploads/2025/05/Cofer_Grey-Market-Regulation.pdf.

Daniel B. Harris. 'China's E-Commerce Law and Its Foreign Company Impacts'. Blog affiliated with a law firm. China Law Blog, Harris Sliwoski LLP, 2019. https://harris-sliwoski.com/chinalawblog/chinas-e-commerce-law-and-its-foreign-company-impacts/.

Dewaya, Muhammad Abdullah. 'Innovation in Islamic Finance: Integrating Blockchain with Maqāṣid al Sharīʿah & Ḥifẓ al Māl'. Journal of Emerging Economies and Islamic Research 13, no. 1 (2025): 1. https://doi.org/10.24191/jeeir.v13i1.3852.

Dr. Michael Tan and Julian Sun. 'China: Legal Framework for e-Commerce'. Law firm publication / Legal insight article. Taylor Wessing – Insights, 22 June 2021. https://www.taylorwessing.com/en/insights-and-events/insights/2021/06/china-legal-framework-for-e-commerce.

Dusuki, Ayraf Wajdi, and Said Bouheraoua. 'The Framework of Maqasid Al-Shari'ah and Its Implication for Islamic Finance'. ICR Journal 2, no. 2 (2011). https://doi.org/10.52282/icr.v2i2.651.

E-Commerce Law 2019, M/126 Royal Decree § Full Text (2019). Enacted under the authority of the Ministry of Commerce.

E-Commerce Law of the People's Republic of China, Order No. 7 of the President of the PRC (13th NPC Standing Committee) Law of the People's Republic of China § Articles 1–89 (2018). https://ipkey.org/en/resources/ip-law-database/details/e-commerce-law-of-the-peoples-republic-of-china. Adopted August 31, 2018; entered into force January 1, 2019.

E-Commerce Law of the People's Republic of China - Chapter 1 General Provisions, Order No. 7 of the President of the PRC (13th NPC Standing Committee) Law of the People's Republic of China § Articles 1–89 (2018). https://www.npc.gov.cn/englishnpc/c23934/202301/28213a0ce3b94d2fb74d9ab236f8e8db.shtml. Adopted on August 31, 2018, by the Standing Committee of the 13th NPC during its 5th session; entered into force January 1, 2019.

Electronic Transactions Law (2007), M/18 Royal Decree (2007). Enacted on 27 March 2007 (corresponding to 8/3/1428H) by Royal Decree No. M/18.

European Commission. Digital Services Act – Questions and Answers. European Commission, 2020. https://fernandezrozas.com/wp-content/uploads/2020/12/Digital_Services_Act___Questions_and_Answers.pdf#:~:text=What%20measures%20does%20the%20legislation,platforms%20will%20have%20to%20react.

European Commission. 'Digital Services Act: Commission Launches Transparency Database'. Official EU Policy

News Release. Digital Strategy – European Commission, 26 September 2023. https://digital-strategy.ec.europa.eu/en/news/digital-services-act-commission-launches-transparency-database.

European Commission. Implementing Regulation Laying down Templates Concerning the Transparency Reporting Obligations of Providers of Online Platforms. POLICY AND LEGISLATION. Directorate-General for Communications Networks, Content and Technology (DG CONNECT), European Commission, 2024. https://digital-strategy.ec.europa.eu/en/library/implementing-regulation-laying-down-templates-concerning-transparency-reporting-obligations.

European Commission. 'The Enforcement Framework under the Digital Services Act'. Official EU policy page. Digital Strategy – European Commission, 2023. https://digital-strategy.ec.europa.eu/en/policies/dsa-enforcement.

European Commission. 'The EU's Digital Services Act'. Policy Overview. Commission – Europe Fit for the Digital Age, 27 October 2022. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en.

European Parliament Research Service. 'Enforcing the Digital Services Act: State of Play'. Epthinktank, 21 November 2024. https://epthinktank.eu/2024/11/21/enforcing-the-digital-services-act-state-of-play/.

Federal Trade Commission. 'What Third Party Sellers Need to Know About the INFORM Consumers Act'. Federal Trade Commission – Business Guidance, 2023. https://www.ftc.gov/business-guidance/resources/what-third-party-sellers-need-know-about-inform-consumers-act.

Gail E. Crawford, Jean-Luc Juhan, Susan Kempe-Mueller, et al. 'Digital Services Act: Practical Implications for Online Services and Platforms'. Latham.London, 14 March 2023. https://www.latham.london/2023/03/digital-services-act-practical-implications-for-online-services-and-platforms/.

Gulyamov, Said. 'Application of Computational Law and Artificial Intelligence Methods for Sharia Compliance Analysis of E-Waste Management Systems Based on Blockchain'. Suhuf: International Journal of Islamic Studies 36, no. 1 (2024): 1. https://doi.org/10.23917/suhuf.v36i1.4447.

Hakami, Ameera. 'An Investigation into the Application of Open-Book Accounting (OBA): A Case Study of Saudi Arabian Companies'. Phd, University of Sheffield, 2023. https://etheses.whiterose.ac.uk/id/eprint/34013/.

Hasan, Asif, Amer Ali Alenazy, Sufyan Habib, and Shahid Husain. 'Examining the Drivers and Barriers to Adoption of E-Government Services in Saudi Arabia'. Journal of Innovative Digital Transformation 1, no. 2 (2024): 139–57. world. https://doi.org/10.1108/JIDT-09-2023-0019.

Hemrit, Wael, and Ines Belgacem. 'Spotlight on Corporate Fraud: How Is Takaful Insurance Stability Affected by Its Disclosure?' Risks 12, no. 9 (2024): 9. https://doi.org/10.3390/risks12090145.

Hidayah, Ahdiyatul, and Nurmu'izzatin Zaharatul Parhi. 'Towards Sharia E-Commerce Regulation: Analysis of Gharar and Consumer Protection in Indonesia'. Saqifah: Jurnal Hukum Ekonomi Syariah 10, no. 1 (2025): 1. https://journals.fasya.uinib.org/index.php/saqifah/article/view/707.

ICLG (International Comparative Legal Guides). 'Digital Business Laws and Regulations - USA'. Text. ICLG, Global Legal Group, 2025. United Kingdom. https://iclg.com/practice-areas/digital-business-laws-and-regulations/usa.

Implementing Regulations of the Anti-Commercial Fraud Law, 155 Ministerial Resolution (2009). Issued by Ministerial Resolution No. 155 dated 6/1/1431H (23 December 2009).

Ishak, Muhammad Shahrul Ifwat, and Nur Syahirah Mohammad Nasir. 'Maqasid Al-Shari'ah in Islamic Finance: Harmonizing Theory and Reality'. The Journal of Muamalat and Islamic Finance Research 18, no. 1 (2021): 108–19. https://doi.org/10.33102/jmifr.v18i1.334.

Islam, Md Sirajul, and Sofiah Samsudin. 'Interpretations of Al-Amanah Among Muslim Scholars and Its Role in Establishing Peace in Society'. Social Change 48, no. 3 (2018). https://doi.org/10.1177/0049085718781689.

Ismail, Hosameldin H., and Rania S. Azab. 'The Role of E-Commerce as an Innovative Solutions in the Development of the Saudi Economy'. Marketing and Management of Innovations 14, no. 4 (2023): 4. https://doi.org/10.21272/mmi.2023.4-19.

Jabbar, Siti Faridah Abdul, and Asma Hakimah Ab Halim. 'The Concept of Fraud in Islamic Law'. In Research Handbook on International Financial Crime. Edward Elgar Publishing, 2015. https://doi.org/10.4337/9781783475780.00039.

Karim, Ridoan, and Imtiaz Mohammad Sifat. 'Treatment of Silence as Misrepresentation in Contracts: A Critical Comparative Analysis of Common Law and Islamic Jurisprudence'. International Journal of Law and Management 60, no. 1 (2018): 69–78. world. https://doi.org/10.1108/IJLMA-08-2016-0073.

Kati Suominen. Implications of the European Union's Digital Regulations on U.S. and EU Economic and Strategic Interests. Center for Strategic & International Studies, 2022. https://www.csis.org/events/implications-eu-digital-services-act-and-digital-markets-act-us-business.

Khan, Ruby. 'Digital Payments: Barrier or Boon for Entrepreneurs' Success - A Case Study of Saudi Arabia'.

International Journal of Advances in Engineering and Management (IJAEM) 5, no. 8 (2023).

Kharusi, Talib Al. 'Towards the Development of a Balanced Legislative Framework for Consumer Data Protection in Electronic Commerce: The Case of the Sultanate of Oman'. Doctoral Thesis (PhD), Technological University Dublin (TU Dublin), 2023. https://arrow.tudublin.ie/sciendoc/271.

Khrais, Laith. 'Bridging Gaps in InsurTech and E-Commerce Integration: Insights from Saudi Arabia'. Insurance Markets and Companies 16, no. 1 (2025): 64–73. https://doi.org/10.21511/ins.16(1).2025.06.

Laney Zhang. 'China: Centralized Internet ID System Officially Launched'. Government legal news and analysis. Global Legal Monitor – Library of Congress, 2025. https://www.loc.gov/item/global-legal-monitor/2025-07-09/china-centralized-internet-id-system-officially-launched/.

Medjedel, Dr Ahmed. 'Digital Marketing in Saudi Arabia: Trends, Challenges, and Opportunities'. Pakistan Journal of Life and Social Sciences (PJLSS) 23, no. 1 (2025). https://doi.org/10.57239/pjlss-2025-23.1.00716.

Miller, Gabby. 'The Digital Services Act Is Fully In Effect, But Many Questions Remain'. Policy analysis / commentary blog. Tech Policy Press, 20 February 2024. https://techpolicy.press/the-digital-services-act-in-full-effect-questions-remain.

Muhammad, Mohd Zulkifli, Fatihah Mohd, Tamrin Amboala, et al. 'Shariah-Compliant E-Payment Framework in Malaysia: Integrating Fiqh, Digital Security and Regulatory Governance'. Journal of Fatwa Management and Research 30, no. 2 (2025): 2. https://doi.org/10.33102/jfatwa.vol30no2.638.

Muneeza, Aishath, and Zakariya Mustapha. 'Blockchain and Its Shariah Compliant Structure'. In Halal Cryptocurrency Management, edited by Mohd Ma'Sum Billah. Springer International Publishing, 2019. https://doi.org/10.1007/978-3-030-10749-9_6.

Nafidzulhaq, Jihad. 'Digital Shariah Compliance Supervision on Stock Market: An Innovative Approach on Islamic Capital Market'. SUKUK: INTERNATIONAL JOURNAL OF BANKING, FINANCE, MANAGEMENT AND BUSINESS 3, no. II (2024): II. https://sukukjournal.org.uk/index.php/sukuk/article/view/47.

Nordin, Nadhirah, Sumayyah Abdul Aziz, Azlin Alisa Ahmad, and Normadiah Daud. 'Contracting with Gharar (Uncertainty) in Forward Contract: What Does Islam Says?' Asian Social Science 10, no. 15 (2014): 15. https://doi.org/10.5539/ass.v10n15p37.

Osman, Ali, and Mohamed Mamdouh. 'The Impact of Government Policies in Middle Eastern Countries on Digital Platform Startups'. Thesis, Massachusetts Institute of Technology, 2024. https://dspace.mit.edu/handle/1721.1/157157.

Ribadu, M. B., A. Mohammed, S. Sa'ad, and K. I. Umar. 'Development and Validation of Sharia Compliance E-Commerce Quality Factors and Measurement Scales'. Savannah Journal of Science and Engineering Technology 1, no. 4 (2023): 4. https://www.sajsetjournal.com.ng/index.php/journal/article/view/60.

Ribadu, Mohammed Bashir, and Wan Nurhayati Wan Ab. Rahman. 'An Integrated Approach towards Sharia Compliance E-Commerce Trust'. Applied Computing and Informatics 15, no. 1 (2019): 1–6. https://doi.org/10.1016/j.aci.2017.09.002.

Ribadu, Mohammed, Wan Nurhayati Wan Ab. Rahman, Abdul Azim Abd Ghani, Azrina Kamaruddin, and Mohd Sukki Othman. 'Sharia Compliance Requirements Framework for E-Commerce Systems: An Exploratory Study'. Journal of Theoretical and Applied Information Technology 98, no. 6 (2020). https://www.academia.edu/79138566/Sharia_Compliance_Requirements_Framework_for_E_Commerce_Systems_An_Exploratory_Study.

Richard Asquith Grey. 'China Imposes Quarterly Platform Seller Reporting - Vatcalc.Com'. Tax policy and VAT compliance news. VATCalc, 26 June 2025. https://www.vatcalc.com/china/china-imposes-quarterly-platform-seller-reporting/.

Rukmanda, Meirani Rahayu, Hasan Bisri, Dedah Jubaedah, Dudang Gojali, and Sholikul Hadi. 'Empowering Sharia-Based Micro, Small and Medium Enterprises (MSMEs) in Indonesia: A Socioeconomic and Ethical Framework for Inclusive Development'. International Journal of Nusantara Islam 13, no. 2 (2025): 2. https://doi.org/10.15575/ijni.v13i2.47733.

'Sahih Muslim 1716a - The Book of Judicial Decisions - كتاب الأقضية - (Ijtihad)'. In Sayings and Teachings of Prophet Muhammad (صلى الله عليه و سلم). n.d. Accessed 3 August 2025. https://sunnah.com/muslim:1716a.

Saied, Aya Hatem. 'The Growth of Digital Marketing for E-Commerce in Saudi Arabia: E-Marketing Strategies of Electronic Commerce Companies in KSA'. International Journal of Business Marketing and Management 9, no. 6 (2024): 11–22. https://www.ijbmm.com/paper/Nov2024/8340436664.pdf.

Shirley Zhang, Yao Lu, and Eunice Ku. 'China's E-Commerce Legislative and Regulatory Framework'. China Briefing, Dezan Shira & Associates, 2013. https://www.china-briefing.com/news/chinas-e-commerce-legislative-and-regulatory-framework/.

Sholikhin, M. Yusron, and R. Nurul Fitri Amijaya. 'E-Commerce Based on the Law of Buying and Selling in Islam'. KnE Social Sciences, 31 March 2019, 1360–70. https://doi.org/10.18502/kss.v3i13.4290.

Terzi, Alessio, Aneil Singh, and Monika Sherwood. Industrial Policy for the 21st Century: Lessons from the Past.

European Economy Discussion Paper No. 157. European Commission, Directorate-General for Economic and Financial Affairs, 2022. https://data.europa.eu/doi/10.2765/538421.

The Need for Privacy Protections: Is Industry Self-Regulation Adequate? (Senate Hearing 112-785): Hearing on S. Hrg. 112-785 before the U.S. Senate Committee on Commerce, Science, and Transportation, United States Senate 112th Congress, 2nd Session (2013). https://www.govinfo.gov/content/pkg/CHRG-112shrg81711/html/CHRG-112shrg81711.htm. Hearing held on June 28, 2012.

Trisha B. Anderson. Geneva Network Comment on Potential U.S. Know Your Business Customer (KYBC) Regulations for Online Services. Position paper / Commentary. Geneva Network, 2021. https://geneva-network.com/research/geneva-network-comment-on-potential-u-s-know-your-business-customer-kybc-regulations-for-online-services/.

Waemustafa, Waeibrorheem, and Sukri Suriani. 'Theory of Gharar and Its Interpretation of Risk and Uncertainty from the Perspectives of Authentic Hadith and the Holy Quran: Review of Literatures'. International Journal of Economic Perspectives 10, no. 1 (2016): 1. http://www.econ-society.org/ijep_contents_10.1.php.

Wahid, Ziadul Ulum, Handoko Budi Prasetiyo, and Tutik Hamidah. 'Ibn Asyur's Concept of Maqashid Al-Shariah and Its Urgency as a Basis for Contemporary Ijtihad'. Fonologi : Jurnal Ilmuan Bahasa Dan Sastra Inggris 3, no. 2 (2025): 14–26. https://doi.org/10.61132/fonologi.v3i2.1674.

World Trademark Review. 'China's New E-Commerce Law - WTR'. 2019. https://www.worldtrademarkreview.com/global-guide/anti-counterfeiting-and-online-brand-enforcement/2019-obe/article/chinas-new-e-commerce-law.

