

Shariah Trustworthiness in Digital Financial Services: A Normative Framework for Shariah Governance and the Prevention of Digital Gharar

Talal Abdullah Hassan Bakhsh^{1*}, Auwal Adam Sa'ad²

¹ PhD Candidate, Institute of Islamic Banking and Finance (IiBF), International Islamic University Malaysia (IIUM), Kuala Lumpur, Malaysia, lahjan@gmail.com

² Institute of Islamic Banking and Finance (IiBF), International Islamic University Malaysia (IIUM), Kuala Lumpur, Malaysia, auwal@iium.edu.my

*Corresponding Author's E-mail: lahjan@gmail.com

Abstract: *Digital financial services expose a limitation in Shariah assessment when approved contracts are delivered through opaque data practices, automated decisions, and interfaces that users cannot readily interpret. Existing accounts consider institutional oversight, operational conduct, and technological uncertainty separately. This paper develops a normative framework for assessing Shariah trustworthiness across these interdependent dimensions. It employs qualitative conceptual analysis and maqasid reasoning, synthesizing scholarship on Islamic financial governance, contractual uncertainty, data stewardship, and algorithmic accountability. The analysis is theoretical and uses illustrative digital financing and payment scenarios rather than observations or survey data. The framework identifies three mutually reinforcing requirements: Shariah data governance, functional Shariah compliance, and prevention of digital gharar. It distinguishes the legal permissibility of a contractual structure from the trustworthiness of the service implementing it. It also shows that technological opacity warrants graduated ethical scrutiny but does not automatically constitute legally prohibited gharar. The framework connects institutional oversight with design controls, meaningful disclosures, reviewable decisions, and remedies. Its contribution is an integrated, operationally oriented account of Shariah trustworthiness without claiming empirical validation. Future assessment can translate these requirements into auditable indicators and test their usefulness across digital financial settings.*

Keywords: Shariah trustworthiness; digital financial services; Shariah data governance; functional Shariah compliance; digital gharar; maqasid al-Shariah; Islamic finance.

1. Article type: Conceptual paper

2. Introduction

The expansion of digital financial services has altered the circumstances in which customers enter, perform and exit financial transactions. Mobile onboarding, automated eligibility decisions, personalized interfaces and continuously updated terms can intervene between a contractual document and the service that a customer actually encounters. These features may enhance access

and efficiency, yet they also distribute information and decision-making authority unevenly between a provider and its users. In Islamic finance, the resulting questions are not exhausted by determining whether the named contract is permissible. They also concern whether the digital implementation preserves the clarity of obligations, safeguards entrusted information and enables participants to understand the economic implications of their decisions.

Shariah governance has traditionally emphasized supervisory expertise, decision-making independence, product approval and continuing institutional review. The Islamic Financial Services Board established principles for such governance arrangements, including proportionality, competence, independence and consistency in oversight (Islamic Financial Services Board, 2009). More recent supervisory guidance reflects the continuing need for accountable governance across different institutional settings (Islamic Financial Services Board, 2025). Neither development implies that contractual validity has become irrelevant. Rather, digital delivery makes it necessary to examine whether approval and oversight reach the operational pathways through which customers actually transact. The distinction matters because a service can satisfy formal disclosure requirements while remaining difficult to understand in practice. An automated financing journey may include accurate contractual clauses but present repayment implications only after several screens, or alter an applicant's eligibility through rules unavailable to the affected person. Such experiences can undermine reasonable reliance without establishing that the underlying contract is automatically invalid. Conversely, technical sophistication or a confusing interface should not be treated as proof of prohibited *gharar* without examining the legally relevant uncertainty and its materiality. A rigorous approach therefore needs to separate the permissibility of the transaction, the quality of implementation and the narrower jurisprudential question of uncertainty affecting contractual rights or exchange.

Contemporary research offers components of this account but commonly examines them from different disciplinary starting points. Islamic fintech scholarship has documented the legal and regulatory implications of technology-enabled finance (Oseni and Ali, 2019). A conceptual assessment of digital risk has connected Islamic financial innovation with the objectives of inclusion and social justice (Alsaghir, 2025). Work on algorithmic governance, meanwhile, explains how computational regulation can change informational control and accountability (Yeung, 2018). The remaining analytical problem is how these insights can be evaluated together without reducing Shariah trustworthiness either to certification or to a generic consumer-confidence score. This paper addresses that problem by proposing Shariah trustworthiness as a normatively assessable quality of a digital financial service. It asks three connected questions: what distinguishes trustworthiness from formal compliance and users' subjective trust; which operational conditions make the concept meaningful in a digital environment; and how can those conditions inform a disciplined assessment of data practices, service functionality and uncertainty? The argument is that trustworthiness should be evaluated through three mutually reinforcing domains: Shariah data governance, functional Shariah compliance and the prevention of digital *gharar*. The paper offers a conceptual derivation and illustrative applications, not a measurement exercise or a claim that the model has been empirically validated.

The contribution has three boundaries. First, it retains legally grounded determinations of permissibility as separate from the graduated assessment of operational trustworthiness. Second, it identifies digital opacity as a potential source of risk that requires further juristic and factual inquiry, rather than equating every design failure with *gharar*. Third, it translates ethical commitments into questions that supervisors and institutions could actually examine. The next sections establish the relevant literature and method, define the model, examine illustrative situations and consider its theoretical and institutional implications.

3. Literature Review

3.1 Shariah governance beyond institutional approval

The institutional foundations of Shariah governance are well developed. Scholarship comparing governance arrangements demonstrates that supervisory structures differ across jurisdictions and that independence, disclosure, competence and operational review are important to their effectiveness (Hasan, 2012). The governance principles of the Islamic Financial Services Board likewise place Shariah oversight within a broader system of responsibility and control, rather than treating a supervisory opinion as the only required mechanism (Islamic Financial Services Board, 2009). For digital services, the question is how these responsibilities follow a product after an initial approval, particularly where software updates, automated rules and outsourced infrastructure can materially influence its operation.

A related strand of scholarship has challenged the tendency to privilege contractual engineering over the economic substance of Islamic financial transactions. El-Gamal argues that assessment should not overlook the substantive function of products behind familiar legal forms (El-Gamal, 2006). This concern is especially relevant when the same nominal agreement can be delivered through different customer journeys and pricing disclosures. The proposal advanced here does not diminish the authority of Shariah supervision; instead, it specifies additional operational questions that supervision should be equipped to ask. A formally authorized financing product remains subject to review when the platform's actual behavior affects the presentation or execution of agreed rights.

Recent conceptual work increasingly addresses the integration of Shariah oversight with digital design. A proposed governance standard for generative artificial intelligence describes oversight across stages of technological development and deployment (Zafar and Ali, 2026). This advances lifecycle accountability, but the question pursued in the present study is wider than one technology. A digital service may create ethically relevant uncertainty through static interface design, automated fee calculations or data sharing even without generative artificial intelligence. The challenge is therefore to establish an evaluative structure applicable to varied digital delivery channels while remaining sensitive to the distinctive legal issues of each product.

3.2 Maqasid, substantive justice and operational evaluation

Maqasid al-Shariah reasoning asks whether practices promote the purposes underlying legal prescriptions, including protection of wealth and the avoidance of unjust harm. A systems approach to these objectives emphasizes relationships between components and their combined effects (Auda, 2008). This perspective is useful for digital services because contractual language, data collection and transaction execution may each appear acceptable in isolation while producing an opaque experience when combined. Maqasid reasoning, however, cannot be invoked as an unrestricted substitute for particular legal rules. Its role here is to orient the assessment, identify questions that require juristic attention and support proportionate remedial recommendations. Studies seeking to operationalize maqasid in Islamic finance provide an important methodological precedent. Monawer and colleagues identify constituent considerations for translating objectives into product design and consumption, showing that an ethical aspiration gains analytical value when connected to specific decisions (Monawer et al., 2022). More generally, the relevance of *maslahah* to organizational responsibility highlights the importance of judging practices in light of actual stakeholder consequences (Dusuki and Abdullah, 2007). The present model follows this movement from principle to reviewable practice, but its distinctive object is the digital service pathway: what the customer is shown, what an automated

system does, and what mechanisms exist when the resulting experience fails to match the approved financial arrangement.

3.3 Digital governance, trust and uncertainty

Outside Islamic finance, standards for financial consumer protection increasingly recognize the consequences of digital delivery for information provision, fair treatment and complaints handling. The updated international principles of financial consumer protection explicitly address digitalization within a general framework of responsible conduct (Organisation for Economic Co-operation and Development, 2022). They are not themselves Shariah standards, but they reveal where operational questions can be specified in a verifiable manner. Likewise, the risk-management framework developed for artificial intelligence supplies a practical example of lifecycle-based governance and documentation (Tabassi, 2023). Such instruments can inform the technical expression of a Shariah evaluation without determining the Islamic legal status of a transaction.

Algorithmic decision systems can make informational asymmetry harder to identify because their rules may be distributed across models, data sources and institutional procedures. Yeung's account of algorithmic regulation distinguishes different configurations of monitoring and control, demonstrating why accountability cannot be reduced to the publication of terms (Yeung, 2018). A customer may receive a legally adequate notice and still have no intelligible account of the action affecting eligibility or cost. Nevertheless, incomplete understanding and prohibited contractual uncertainty are not interchangeable. Materiality, the relevant rights and obligations, the nature of the transaction and the available information must be examined before reaching a juristic conclusion.

This review identifies an integration problem rather than an absence of earlier work. Governance scholarship addresses institutional authority; maqasid scholarship clarifies ethical purposes; and digital regulation scholarship attends to the operation of technological systems. What remains under-specified is how to distinguish a service's objective entitlement to trust from both formal permissibility and the subjective confidence of its users. An integrated model can make that distinction useful if it specifies independently reviewable conditions, clarifies how they interact and avoids conflating normative risk with established legal prohibition.

4. Research Methodology

This study adopts qualitative conceptual analysis and normative synthesis. Its object is not the prevalence of a phenomenon among institutions or users, but the conditions under which a digitally delivered Islamic financial service can reasonably be assessed as deserving trust. The source base comprises established scholarship on Islamic financial jurisprudence and Shariah governance, conceptual research on maqasid and Islamic fintech, and published governance principles addressing financial consumer protection and computational systems. The analysis uses these materials to refine terms, compare normative concerns and derive an integrated evaluative model. It is neither a systematic literature review nor an empirical study, and no statistical dataset, interview sample, fieldwork period or institutional case series was collected.

The analytic sequence consists of four operations. First, the study separates four constructs that are often placed together: contractual permissibility, institutional legitimacy, perceived trust and trustworthiness. Second, it identifies recurring concerns about entrusted data, the functional delivery of obligations and uncertainty in user-facing transactions. Third, it evaluates those concerns against the objectives of transparency, fairness, protection of wealth and prevention of avoidable harm,

without presuming that each ethical concern constitutes a legal violation. Fourth, it synthesizes the concerns into three review domains and applies the resulting framework to explicitly hypothetical scenarios. These operations are a transparent account of conceptual reasoning, not a claim to a formal coding procedure or exhaustive retrieval protocol that was never carried out.

The framework is judged by conceptual criteria rather than observed outcomes: definitional clarity, distinctiveness of domains, correspondence between proposed indicators and normative concerns, internal coherence, and applicability without unsupported factual assumptions. Competing interpretations are considered where important, particularly the difference between operational opacity and the technical legal conditions of *gharar*. Normative propositions developed through this method remain open to subsequent legal evaluation and empirical testing. The examples below are analytical stress tests, not evidence that particular firms use the described practices.

5. Conceptual and Theoretical Foundations

5.1 Compliance, legitimacy, trust and trustworthiness

Shariah compliance refers, in the present analysis, to conformity with relevant Islamic legal requirements governing the structure and performance of a financial transaction. An appropriately constituted supervisory decision is important evidence of institutional processes for pursuing this conformity, but cannot establish every later fact about the implementation of a software-enabled service. Institutional legitimacy concerns the recognized authority and acceptability of the provider and its governance arrangements. Perceived trust is an attitude held by users, which may be influenced by branding, previous experience or recommendations and may therefore be misplaced. Trustworthiness differs from all three: it concerns whether the service has features that justify reliance on its lawful, transparent and accountable operation.

This distinction has two consequences. A technically attractive platform is not rendered Shariah-compliant because users trust it; confidence cannot replace legal assessment. Equally, contractual compliance should not be interpreted as conclusive proof that every associated information practice or interface design is fair. The model therefore treats formal permissibility and operational trustworthiness as related but non-identical objects of inquiry. Legal prohibitions establish constraints that a service must satisfy; within and beyond those constraints, different levels of accountable performance may be identified without inventing degrees of lawful or unlawful status.

5.2 Normative foundations and their limits

Three connected foundations support the proposed construct. Shariah governance supplies institutional roles for scrutiny, challenge, monitoring and correction. Maqasid reasoning supplies a perspective for considering substantive consequences, particularly the preservation of wealth, justice and avoidance of preventable harm. A systems-oriented account of digital finance explains why outcomes emerge through the interaction of data, algorithms, workflow rules, interfaces and oversight. Auda's systems treatment of maqasid helps justify attention to such interactions rather than isolated controls (Auda, 2008). The theoretical move is to locate normative responsibility at points where institutional decisions become technical behavior experienced by users. The model does not claim that transparency is unlimited or that all uncertainty is impermissible. Financial products may involve lawful commercial risk, and certain decision criteria legitimately remain protected for security or anti-fraud reasons. The relevant requirement is an appropriate degree of intelligibility and reviewability, taking account of the purpose of the information, the customer's obligations and the

risk of harm. Likewise, the juristic assessment of gharar depends on established rules regarding the relevant contract, the degree and effect of uncertainty and the rights at stake. The model is intended to identify and organize such questions; it cannot settle every disputed jurisprudential issue merely by labeling a practice digital.

5.3 A cumulative but non-substitutive construct

Trustworthiness is cumulative because weaknesses in data management, operational functionality and uncertainty prevention can interact to aggravate risk. A provider could explain its fees clearly but use customer information in ways inconsistent with informed consent; another could protect data effectively while presenting contractual obligations through misleading sequences. Strong performance in one domain does not erase a serious defect in another. At the same time, the three domains are analytically distinguishable: data governance asks how information is stewarded; functional compliance asks whether the approved arrangement is implemented faithfully; and prevention of digital gharar asks whether consequential uncertainty is created, obscured or left unaddressed.

The framework is therefore not an additive score or a claim that three measures have equal empirical weights. It offers a structured judgement in which foundational legal requirements are assessed first, followed by evidence of operational design and accountability. This avoids turning a normative model into an unsupported numerical index. A future scoring instrument could be developed, but would require expert validation, evidence of measurement properties and clear treatment of non-compensable legal failures.

6. Proposed Normative Framework for Shariah Trustworthiness

6.1 Shariah data governance

The first domain concerns the treatment of customer and transaction information as an entrusted resource with financial consequences. Digital providers collect information to establish identity, prevent fraud, assess suitability, set eligibility conditions and provide services. The normative questions concern purpose limitation, proportionality, informed authorization where applicable, data quality, accountable sharing and accessible avenues for correction. The framework does not infer that all data processing requires identical forms of consent or that legitimate regulatory obligations can be displaced by customer preference. It asks whether the institution can explain what information is used, why it is used, who is accountable and how foreseeable misuse is prevented.

Data governance becomes specifically relevant to Islamic finance when information practices affect lawful financial access, the fairness of treatment or the meaningfulness of participation. An algorithmic categorization that produces unexplained differences in service access raises questions about appropriate review, even if no discriminatory conduct is established. The international consumer-protection principles provide a complementary reference for fair conduct and responsible digital disclosure (Organisation for Economic Co-operation and Development, 2022). Within the present framework, the Shariah dimension emerges from the relationship between those operational practices and the duties of trust, justice and protection from harm. The indicators proposed for later assessment include the presence of documented data purposes, access controls, accountable third-party arrangements, mechanisms for correcting consequential inaccuracies and reasons for decisions at an appropriate level of explanation. They are assessment questions rather than findings about existing providers. Strong governance requires evidence from actual data flows and institutional

records, not merely the appearance of a privacy statement. It also requires supervision to revisit the data consequences of changing software or commercial partnerships where those changes are material to the approved service.

6.2 Functional Shariah compliance

The second domain tests the relationship between a Shariah-approved financial arrangement and its implementation. Contractual obligations are communicated and performed through particular screens, calculations, transaction states, reminders and automated decision rules. A service can introduce implementation risk if a displayed payment schedule diverges from its contractual basis, if a fee is applied inconsistently, or if a user is asked to assent before receiving information necessary to understand the commitment. These are functional questions requiring factual examination; they cannot be resolved solely by inspecting a standard contract template. An institutional audit should therefore trace important obligations through the entire customer journey: product configuration, precontractual disclosure, consent, execution, payment administration, amendments, complaint handling and closure. The relevant test is whether the system behaves consistently with the approved structure and whether deviations are detectable and correctable. Recent work on integrating objectives of Islamic law into operational auditing illustrates the value of treating substantive accountability as an ongoing institutional practice (Sulistiyowati et al., 2026). The present model extends that concern to the actual interaction between digital rules and the customer.

The phrase compliance by design describes the governance aspiration, not a claim that coding replaces jurisprudential judgement. It means that the development process should specify relevant Shariah requirements as verifiable controls, assign ownership for monitoring, document the conditions under which code changes require review and provide an escalation path when behavior departs from the approved design. Technical teams can confirm implementation facts; qualified Shariah authorities determine their normative significance. Neither group can responsibly substitute for the other.

6.3 Prevention of digital gharar

The third domain examines uncertainty generated or amplified by digital delivery. Classical discussion of gharar addresses uncertainty with legal relevance to contractual exchange rather than the elimination of every ordinary commercial risk. El-Gamal's analysis of Islamic finance emphasizes the importance of the substantive economic implications of transaction structures (El-Gamal, 2006). Within digital delivery, uncertainty can arise when essential costs are difficult to identify, economically consequential terms are hidden behind interface layers, or rules affecting obligations change without adequate notice. These situations justify inquiry because customers may be unable to identify the bargain to which they are committing or foresee the effect of taking a particular action.

For precision, this paper uses digital gharar as an analytical label for potential gharar-related concerns arising through digital systems, not as a declaration that a new autonomous category of prohibition has been established. There is a necessary distinction between three conditions: ordinary technical complexity, ethically troubling opacity and uncertainty sufficient to engage the legal doctrine of gharar in a particular transaction. Only the last warrants a definitive legal classification, and its assessment requires the relevant doctrinal tests and facts. A confusing interface may be ethically problematic without invalidating an otherwise clear agreement; a materially undisclosed obligation may require more serious consideration. This graded diagnostic logic protects the term from being extended beyond its jurisprudential foundation.

Potential safeguards include clear presentation of financial obligations before commitment, understandable explanations of consequential automated outcomes, change notifications proportionate to their effects, consistent treatment of fees and accessible human review where a decision materially affects rights. These measures are not interchangeable with formal disclosure: a long document may meet a disclosure formality while failing to support meaningful comprehension. Equally, a concise interface cannot eliminate the need for complete enforceable terms. The aim is congruence between legal clarity, operational predictability and the customer's reasonable opportunity to understand the decision.

6.4 Integration, thresholds and review sequence

The three domains form a connected assessment rather than three independent certificates. Data can determine eligibility; eligibility rules can shape the functional performance of a contract; and unexplained performance can generate uncertainty about obligations. A proper review should first establish the contractual arrangement and the applicable legal requirements, then map the digital functions responsible for implementing it, trace the data used at decisive points and examine whether relevant financial consequences are intelligible. Where an observed practice raises possible gharar, the concern should be referred for a transaction-specific juristic evaluation rather than presumed unlawful by the assessor. The matrix below sets out review questions that follow from this logic. It intentionally uses no numerical thresholds because neither empirical weights nor universal juristic cut-offs are established by the conceptual method. It is possible to distinguish a satisfactory documented control, a weakness requiring remediation and a potentially material Shariah question needing authoritative review, but those assessments must remain grounded in the actual product and jurisdiction. A high-level governance indicator cannot override a clearly established legal prohibition.

Table 1. Proposed domains and diagnostic questions for assessing Shariah trustworthiness

Review domain	Reviewable criteria	Possible escalation trigger
Shariah data governance	Documented purpose, proportionate processing, accountable sharing, correction and access controls	Consequential data use cannot be traced or adequately explained
Functional Shariah compliance	Agreement–system alignment, transparent costs, controlled changes and tested transaction pathways	Execution or disclosed obligations depart materially from approved terms
Prevention of digital gharar	Intelligible economic terms, predictable obligations, timely notifications and accessible review	Potentially material uncertainty concerning the rights or subject matter of an exchange

7. Illustrative Analytical Application

7.1 Automated financing eligibility

Consider a hypothetical platform offering Islamic consumer financing. The approved agreement identifies the asset, price, payment schedule and responsibilities, while an automated eligibility system determines which applicants can proceed. Applicants receive different outcomes after similar onboarding journeys, but the provider gives only a generic rejection message and offers no route for correcting information. The contractual structure might remain sound; nonetheless, the data-governance domain would ask whether records are accurate and the relevant processing is accountable. Functional compliance would examine whether automated rules alter approved

conditions. The uncertainty domain would ask whether a lack of explanation affects the person's understanding of a contractual obligation or instead concerns precontractual eligibility alone.

The example illustrates why these questions should not be merged. A rejection before a contract exists ordinarily calls for scrutiny of fairness and data practice, not an automatic finding of gharar in a non-existent exchange. By contrast, a hidden algorithmic adjustment to an already agreed payment obligation could raise distinct contractual questions. A Shariah committee and technical reviewers would need evidence about the product, system events and legal relationship before deciding whether the issue concerns ethical quality, operational breach or impermissible uncertainty. The framework's value is its discipline in distinguishing these paths, rather than the production of a definitive verdict from limited facts.

7.2 Digital payments and information sharing

A second hypothetical service processes Islamic digital payments and uses transaction histories to personalize offers from affiliated providers. The data-governance assessment would ask whether this secondary use is properly authorized and explained, whether users can exercise applicable controls and whether the sharing is necessary for a legitimate purpose. Functional compliance would examine whether additional charges, exchange conditions or payment execution differ from the approved service. The digital-gharar inquiry would be narrower: does the opacity of any relevant term create uncertainty about the financial exchange itself, or does it primarily raise a separate concern about information stewardship? Here the concept of trustworthiness prevents two oversimplifications. The provider should not claim that the legality of the payment contract settles every concern about downstream profiling. Conversely, concern about profiling does not establish that the payment contract contains prohibited gharar. The domains jointly support an informed overall assessment while preserving the separate reasoning needed for particular legal determinations. This distinction is consistent with the wider regulatory need to document technical risks and specify accountability throughout system use (Tabassi, 2023).

7.3 Implications of the illustrative comparison

Both scenarios show that a binary contract-level approval can coexist with different operational profiles. They also show that the proposed model is not a general argument against automation, profiling or complex products. Its assessment is conditional on context, materiality, the ability to correct errors and the relationship between a technical practice and the rights or obligations of participants. The scenarios are illustrative constructions and do not represent observations, survey findings or evidence of prevalence. Their purpose is to test whether the model separates concepts that would otherwise be prematurely conflated.

8. Discussion and Implications

The framework contributes to governance theory by locating trustworthiness in the continuing relationship between institutional authority and the operation of a digital service. Traditional approval remains a necessary source of legal assurance, but a technology-enabled service may change in ways that a static approval cannot fully anticipate. The model therefore treats oversight as a continuing responsibility to examine material technical changes, investigate mismatches between approved terms and performed outcomes, and connect customer-facing evidence with Shariah review. Lifecycle governance developed for artificial intelligence offers an analogous recognition of responsibility

across development and deployment, although its rules cannot independently determine Shariah validity (Zafar and Ali, 2026).

The model's second contribution is terminological restraint. Much discussion of digital trust combines perceptions, institutional reputation, legal approval and actual safeguards within one broad term. By distinguishing them, the study avoids assuming that visible confidence proves normative adequacy or that a lawful contract guarantees a good digital experience. It also resists a competing error: converting every experience of opacity into a prohibited form of *gharar*. *Gharar* is preserved as a jurisprudential concept whose application depends on the relevant transaction and degree of uncertainty. Digital-system analysis can identify facts that are pertinent to that evaluation, but it does not dispense with juristic reasoning.

The third contribution is methodological. Rather than presenting a new index without measurement evidence, the framework offers a sequence of questions that could later be translated into assessments with documented evidentiary standards. Researchers could distinguish indicators observed through interface inspection, internal audit evidence and user comprehension studies. They could then investigate whether the domains are empirically separable, whether knowledgeable Shariah reviewers agree on classifications and which weaknesses most strongly affect user outcomes. Future research could also compare different forms of financing, payment and savings products, or evaluate how different jurisdictions assign responsibility for outsourced and automated functions. These are prospective research opportunities rather than results claimed here.

For supervisors and standard-setting organizations, the practical implication is to consider whether existing Shariah governance expectations reach consequential changes in data use, software rules, disclosures and complaint resolution. The Islamic Financial Services Board's newer supervisory principles emphasize effective oversight while acknowledging differences between jurisdictions, an approach compatible with proportionate implementation (Islamic Financial Services Board, 2025). The present paper does not prescribe a universal technology rule or a replacement for local law. It identifies review questions whose materiality will vary with product risk and governance arrangements. For Shariah boards, the framework supports collaboration with personnel who understand data flows, automated decision-making and software controls. The board should not need to perform software engineering, but it must be able to request intelligible evidence of how an approved financial arrangement is implemented. Relevant controls include documented product rules, change logs, exception handling, reproducible fee calculations, clear contractual disclosure and routes for escalating unresolved user complaints. Technical experts, in turn, need sufficiently precise normative requirements to make implementation testable rather than relying on general statements of fairness.

For institutions, the model suggests assessing trustworthiness at critical points in the service journey instead of relying only on annual policy reviews. Design decisions made during onboarding and consent, the communication of prices and repayments, eligibility assessment, transactions and amendments can affect different domains simultaneously. A risk-based review should prioritize decisions with material consequences for rights, wealth or access. An institution may use the model diagnostically even where it has not adopted a numerical measure. Documenting why a practice is judged acceptable, uncertain or in need of correction would be more defensible than assigning an unexplained composite score. Three limitations constrain interpretation. First, the paper is conceptual and does not establish that the proposed dimensions predict user behavior, institutional performance or Shariah non-compliance in a population. Second, it is not a comparative legal opinion: particular determinations may differ across products, authorities and schools of jurisprudence. Third, available technical protections and duties of disclosure change with the jurisdiction and the service. The

framework therefore requires contextual judgment and future testing before it can serve as a validated supervisory instrument. These boundaries do not remove its analytical relevance; they define what the normative argument can responsibly support.

9. Conclusion

Digital delivery complicates the evaluation of Islamic financial services because the customer experiences a combination of contractual terms, data practices, automated rules and interface choices. This paper has developed a normative account of Shariah trustworthiness that joins Shariah data governance, functional Shariah compliance and prevention of digital gharar without collapsing them into one category. Its central distinction is between the legal permissibility of a contract and the continuing operational quality of the service through which it is delivered. The framework also clarifies that technologically generated opacity may justify scrutiny without, by itself, proving legally prohibited gharar. The proposed approach can guide questions asked during product design, ongoing oversight and review of consequential digital changes. It does not claim empirical validation or offer universal weights and legal thresholds. Its next step is disciplined operationalization: specialist juristic review of context-specific uncertainty, the development of observable indicators and comparison with documented service outcomes. Such work can test whether the framework provides a useful bridge between Islamic legal principles and accountable digital financial practice.

References

- Alsaghir, M. (2025), 'Digital risks and Islamic FinTech: a road map to social justice and financial inclusion', *Journal of Islamic Accounting and Business Research*, Vol. 16 No. 7, pp. 1265–1282, <https://doi.org/10.1108/JIABR-10-2022-0262>.
- Auda, J. (2008), *Maqasid Al-Shariah as Philosophy of Islamic Law: A Systems Approach*, International Institute of Islamic Thought, London, <https://doi.org/10.2307/j.ctvkc67tg>.
- Dusuki, A.W. and Abdullah, N.I. (2007), 'Maqasid al-Shari'ah, maslahah, and corporate social responsibility', *American Journal of Islamic Social Sciences*, Vol. 24 No. 1, pp. 25–45, <https://doi.org/10.35632/ajis.v24i1.415>.
- El-Gamal, M.A. (2006), *Islamic Finance: Law, Economics, and Practice*, Cambridge University Press, Cambridge, <https://doi.org/10.1017/CBO9780511753756>.
- Hasan, Z. (2012), *Shari'ah Governance in Islamic Banks*, Edinburgh University Press, Edinburgh, <https://doi.org/10.1515/9780748645596>.
- Islamic Financial Services Board (2009), *Guiding Principles on Shari'ah Governance Systems for Institutions Offering Islamic Financial Services (IFSB-10)*, Islamic Financial Services Board, Kuala Lumpur, https://www.ifsb.org/wp-content/uploads/2023/10/IFSB-10-December-2009_En.pdf.
- Islamic Financial Services Board (2025), *Guiding Principles for Effective Supervision of Shari'ah Governance (IFSB-31)*, Islamic Financial Services Board, Kuala Lumpur, <https://www.ifsb.org/wp-content/uploads/2025/07/IFSB-31-Guiding-Principles-for-Effective-Supervision-of-Shariah-Governance.pdf>.
- Monawer, A.T.M., Abdul Rahman, N.N., Qasem Al-Nahari, A.A.A., Haji Abdullah, L., Ali, A.K. and Meguellati, A. (2022), 'The actualization of maqasid al-Shari'ah in Islamic finance: a

- conceptual framework', *International Journal of Islamic and Middle Eastern Finance and Management*, Vol. 15 No. 5, pp. 847–864, <https://doi.org/10.1108/IMEFM-06-2020-0293>.
- Organisation for Economic Co-operation and Development (2022), *G20/OECD High-Level Principles on Financial Consumer Protection 2022*, OECD Publishing, Paris, <https://doi.org/10.1787/48cc3df0-en>.
- Oseni, U.A. and Ali, S.N. (Eds) (2019), *Fintech in Islamic Finance: Theory and Practice*, Routledge, Abingdon.
- Sulistyowati, S., Daud, D. and Kasim, E.S. (2026), 'Reframing operational auditing in Islamic banks: a conceptual framework based on Maqasid Shariah and Islamic agency theory', *Journal of Islamic Accounting and Business Research*, advance online publication, <https://doi.org/10.1108/JIABR-07-2025-0458>.
- Tabassi, E. (2023), *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, NIST AI 100-1, National Institute of Standards and Technology, Gaithersburg, MD, <https://doi.org/10.6028/NIST.AI.100-1>.
- Yeung, K. (2018), 'Algorithmic regulation: a critical interrogation', *Regulation & Governance*, Vol. 12 No. 4, pp. 505–523, <https://doi.org/10.1111/regg.12158>.
- Zafar, M.B. and Ali, H. (2026), 'Shariah governance standard on generative AI for Islamic financial institutions', *Journal of Islamic Accounting and Business Research*, advance online publication, <https://doi.org/10.1108/JIABR-03-2025-0141>.