

Operationalizing Shariah Governance in Islamic FinTech Platforms in Saudi Arabia: A Normative and Institutional Framework

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: *Islamic financial technology platforms in Saudi Arabia face a governance challenge when approved Shariah requirements are translated into automated transactions, digital disclosures, and changing software systems. Institution centered oversight does not fully explain how compliance should be assured throughout these operational processes. This study develops a normative and institutional framework for continuous Shariah governance in digital financial services. It uses conceptual theory building to synthesize institutional theory, Maqasid al-Shariah, Islamic financial governance scholarship, research on algorithmic oversight, and publicly available Saudi regulatory documents. The analysis distinguishes governance authority from technical enforcement and operational evidence without collecting primary data or testing outcomes. The proposed framework specifies five connected layers: institutional governance, Shariah governance, technology and regulatory technology, operational compliance, and governance outcomes and legitimacy. It identifies authorization traceability, controlled system changes, exception monitoring, and corrective feedback as mechanisms linking approved decisions to platform operations. Ten preliminary indicators support future examination of governance implementation without claiming empirical validation. The framework contributes an operational lifecycle architecture that distinguishes enabling controls from their evaluative outcomes. Its application may guide proportionate platform assurance and future independent empirical assessment of Shariah compliance and meaningful customer protection.*

Keywords: Islamic financial technology; Shariah governance; operational compliance; Saudi Arabia; regulatory technology; institutional legitimacy; Maqasid al-Shariah.

1. Introduction

Digital financial services increasingly combine customer-facing interfaces, automated contractual workflows, data-driven decisions, and outsourced technical infrastructure. Such arrangements change not only how financial services are distributed but also where decisions affecting customers are made and recorded. Research on financial technology identifies the interaction of technological innovation, new intermediation models, and changing organizational boundaries as a defining feature of contemporary financial services (Gomber et al., 2018). For Islamic financial services, these characteristics create an additional question: how can Shariah obligations remain effective when an

approved contract is translated into software rules, transaction sequences, disclosures, and automated decisions? Shariah governance is not a substitute for financial regulation, nor is regulatory compliance sufficient to establish Shariah conformity. The relevant accountability systems overlap without being identical. A product may receive appropriate initial Shariah review yet still be implemented through an interface that obscures key contractual information, a transaction workflow that departs from approved sequencing, or software revisions that change the manner of execution. These examples identify possible control failures rather than findings about the prevalence of misconduct in Saudi platforms. They indicate why Shariah assurance requires attention to the operation of services as well as to their formal legal design.

Saudi Arabia offers a particularly consequential institutional context. The Saudi Central Bank established a formal Shariah governance framework for local banks conducting Islamic banking activities, specifying responsibilities for boards, management, Shariah committees, and internal control functions (Saudi Central Bank, 2020). Subsequently, it introduced specific disclosure requirements for banks conducting Shariah-compliant banking, effective at the end of 2024 (Saudi Central Bank, 2024). These measures demonstrate that the Saudi environment is not devoid of Shariah governance rules. Their banking-specific scope also means that the requirements applicable to a particular financial technology platform cannot be inferred merely from the fact that it offers an Islamic product.

Digital activity spans different regulated business models. Securities-related experimentation and authorization fall within the Capital Market Authority's remit, while other financial services may be supervised by the Saudi Central Bank. In 2025, the Capital Market Authority approved a framework allowing appropriately licensed capital market institutions to arrange debt-instrument offerings through securities crowdfunding platforms outside the earlier experimental-permit route (Capital Market Authority, 2025). Governance design must therefore begin with the actual regulated entity, financial activity, contractual relationship, and allocation of responsibility across operators and technical providers. The theoretical problem is more specific than a general call for additional Shariah oversight. Traditional institutional arrangements emphasize decision-making authorities, review mandates, competence, independence, and reporting. Those elements remain indispensable, but their existence does not by itself explain how a Shariah decision becomes an enforceable platform rule, how changes are detected, or how operational exceptions return to the relevant authority. Islamic banking research establishes the significance of governance structures while largely examining institutions rather than the detailed configuration of digital workflows (Nomran & Haron, 2020). The unresolved issue concerns the translation between governance authority and the technological execution of financial services.

This article asks: How can Shariah governance be operationalized in Islamic financial technology platforms in Saudi Arabia so that institutional accountability, Maqasid al-Shariah, regulatory expectations, and day-to-day platform operations remain connected? Its objective is to develop an analytically specified and context-sensitive normative framework, not to estimate the effectiveness of Saudi platforms. The study combines institutional theory, Maqasid-oriented normative reasoning, Islamic finance governance scholarship, and research on algorithmic regulation in a structured conceptual synthesis. The contribution has three dimensions. Conceptually, the article defines operational Shariah governance as the continuing translation, monitoring, escalation, and revision of approved Shariah requirements throughout a platform's service lifecycle. Architecturally, it distinguishes four enabling governance layers from a fifth layer representing outcomes and legitimacy, while identifying downward authorization and upward assurance mechanisms. Operationally, it connects each layer to preliminary indicators and falsifiable propositions that can inform later empirical work. The paper proceeds from theoretical foundations and a critical synthesis

to a transparent conceptual method, framework architecture, Saudi institutional application, and implications.

2. Theoretical Foundations

2.1 Institutional legitimacy and the problem of decoupling

Institutional theory explains why organizations adopt governance arrangements that signal conformity with external rules, professional expectations, and accepted organizational practices. Meyer and Rowan (1977) argued that formal structures can become decoupled from actual activities when organizations prioritize legitimacy without ensuring operational correspondence. Applied to Islamic financial technology, this possibility highlights a distinction between possessing a Shariah governance structure and demonstrating that each relevant digital transaction is executed consistently with the decisions of that structure. The point is a theoretical risk of decoupling, not evidence that such decoupling is widespread in Saudi Arabia. The literature on institutional isomorphism also shows how coercive, normative, and mimetic pressures influence organizational behavior (DiMaggio & Powell, 1983). For a regulated Islamic financial platform, coercive pressures may arise from applicable supervisory requirements, normative pressures from Shariah practitioners and professional standards, and mimetic pressures from governance models used by comparable firms. A platform can respond to these pressures through policies and committees; however, operational legitimacy additionally requires control evidence linking those arrangements to software configuration and business processes. This distinction provides a theoretical reason to examine design, execution, and assurance as connected institutional practices.

Scott's institutional perspective distinguishes regulatory, normative, and cultural-cognitive sources of legitimacy (Scott, 2013). In Islamic financial technology, the regulatory pillar concerns legally applicable requirements and supervisory accountability; the normative pillar concerns Shariah decisions, ethical duties, and professional standards; and the cultural-cognitive pillar concerns users' expectations of what it means for a service to be genuinely Shariah-compliant. These pillars cannot be collapsed into one certification. A platform may be legally licensed yet need a separate basis for a Shariah claim, while user confidence may depend on trustworthy explanations and observable remediation when errors occur. An operational approach responds by making accountability traceable. It asks who approved a transaction rule, how that rule was implemented, which changes may affect it, which events were monitored, and who can suspend or remediate an exception. Institutional legitimacy thereby becomes connected to evidence that formal governance decisions are enacted in ordinary transactions rather than merely described in policies. Such traceability can also expose disagreement between technical personnel, Shariah advisers, and management before it develops into a broader accountability failure.

2.2 Maqasid al-Shariah as a normative evaluative lens

Maqasid al-Shariah introduces a complementary question: does a formally acceptable financial process advance or undermine the purposes that justify its acceptability? Auda (2008) advances a systems-oriented understanding of the objectives of Islamic law that foregrounds purpose, interaction, and the consequences of legal reasoning. Within financial platforms, these ideas direct attention to the practical treatment of customers, the intelligibility of contractual choices, the protection of wealth, and the prevention of avoidable harm. Maqasid reasoning does not authorize the disregard of specific contractual requirements; rather, it informs evaluation within the boundaries of applicable Shariah determinations. This distinction is essential for platform governance. A digital interface can display

legally relevant terms, but the ordering, visibility, and timing of those terms may influence whether users can exercise meaningful understanding and choice. Similarly, a compliant product architecture may be compromised by unauthorized configuration changes or poorly controlled exception handling. The normative assessment therefore considers both the validity of the underlying transaction and the way the customer encounters and completes it. Transparency, fairness, accountability, and protection are evaluated as operational aims rather than as automatically achieved outcomes.

Operationalization requires resisting two opposite simplifications. It would be inadequate to equate Shariah conformity with a single aggregate ethical score, because some legal requirements involve non-substitutable conditions. It would also be inadequate to treat formal contractual approval as exhausting the governance question, because execution and disclosure can introduce distinct problems. Accordingly, the framework places Shariah determination and oversight in a dedicated layer while treating Maqasid alignment as a cross-cutting normative criterion for control design and outcome assessment. Disagreement over a Shariah ruling must be handled through competent, authorized processes, not delegated to an algorithm.

2.3 Shariah governance: oversight, independence, and operational assurance

The established literature identifies specialist oversight, independence, transparency, and internal assurance as important elements of Shariah governance. Grais and Pellegrini (2006) analyze how internal Shariah supervisory arrangements relate to compliance within institutions offering Islamic financial services. Their analysis explains why Shariah competence and a credible reporting line remain important even when technology supplies evidence and automated alerts. Governance technology is an instrument of responsible oversight, not a replacement for authorized interpretation. Comparative research identifies variation in the institutions and procedures through which Shariah governance is conducted across jurisdictions (Hasan, 2011). This variation cautions against assuming one universally applicable governance arrangement. In Saudi Arabia, the relevant legal and supervisory obligations depend on the license and activity concerned. A normative platform architecture may supply design principles across business models, but it must leave intact the jurisdiction-specific allocation of final Shariah, compliance, risk, and supervisory responsibilities.

Research on Islamic bank governance shows that governance structures can matter to institutional behavior and financial outcomes (Mollah et al., 2017). Yet relationships estimated for banks cannot be imported as evidence that a proposed control system improves outcomes in an untested digital platform. The present study therefore identifies plausible mechanisms and indicators, while explicitly reserving assertions of effectiveness for future validation. Such methodological restraint is particularly important when the proposed framework is intended to inform policy rather than merely organize concepts.

2.4 Algorithmic governance and regulatory technology

Digital finance changes the location of operational discretion. Some decisions are encoded in eligibility rules, event-triggered workflows, automated notifications, and exception thresholds before individual transactions occur. Yeung (2018) explains how algorithmic regulation can combine continual data collection, monitoring, and feedback while also generating new legitimacy concerns. This insight supports a dual view of regulatory technology: it can strengthen the observability of operations, but poorly designed automation can also obscure discretion and intensify dependence on unexamined system rules. Regulatory innovation scholarship stresses that financial technology requires approaches that balance innovation, accountability, and differentiated supervisory risks

(Zetzsche et al., 2017). From a Shariah governance perspective, the analogous task is to convert normative obligations into appropriately scoped technical controls without reducing jurisprudential judgment to software output. Automated systems can check whether configured steps occur, whether mandatory disclosures appear, or whether an exception has been escalated. They cannot establish the authoritative permissibility of a novel contractual structure independently of qualified Shariah review.

The resulting theoretical synthesis joins three functions: institutional theory explains why accountable governance must be demonstrable; Maqasid al-Shariah supplies criteria for judging the substance and consequences of conduct; and digital governance explains how continuing evidence may be captured and acted upon. Operational Shariah governance occupies their intersection. It is defined here as a system of authorized Shariah interpretation, control specification, monitored execution, exception resolution, and periodic reassessment embedded in the lifecycle of platform-delivered financial services.

3. Critical Literature Synthesis and Research Gap

3.1 Institution-centered Shariah governance

The institutional Shariah governance literature develops an important foundation of committee responsibility, independence, audit, and organizational accountability. The Islamic Financial Services Board (2009) offers guiding principles for Shariah governance systems that emphasize an appropriate governance structure, competence, independence, confidentiality, and consistency. These principles create a governance baseline for Islamic financial institutions, but their generality leaves the design of platform-level technical controls to the entity and its relevant supervisory environment. A review of research connecting Shariah governance arrangements to Islamic bank performance illustrates the empirical emphasis on institutional characteristics and outcomes (Nomran & Haron, 2020). This scholarship is valuable for governance legitimacy but does not directly specify an operational path between a ruling, a software release, a transaction event, and an independent assurance report. That absence is a limitation of the literature's predominant unit of analysis rather than a failure of its authors to anticipate every digital service.

3.2 Islamic financial technology and emerging governance risks

Financial technology research explains innovation through changes in ecosystems, business models, user interactions, and technological infrastructures (Lee & Shin, 2018). Islamic financial technology scholarship adds the requirement that innovation remain compatible with Shariah commitments and a broader ethical conception of finance. Hassan et al. (2020) discuss how financial technology may support adaptation and resilience in Islamic finance while also creating new implementation challenges. Such scholarship establishes why the domain matters, but the operational mapping from Shariah authorization to code-level controls remains comparatively less developed. More recent conceptual work directly addresses this intersection. Mohd Najib et al. (2026) propose a risk-based Maqasid Shariah governance framework for Islamic financial technology that brings Shariah and technological risks within an integrated perspective. The existence of this work makes it untenable to claim that no conceptual framework connects Islamic financial technology, governance, and Maqasid principles. The narrower contribution developed here is a lifecycle-oriented operational architecture that separates institutional authority, Shariah determination, technical enforcement, transaction-level compliance, and outcomes, and identifies the evidence that must circulate between these layers.

This distinction is substantive rather than terminological. A risk-based framework may identify relevant categories of threat and response. An operational architecture additionally asks how an approved rule enters production, who can change it, how exceptions are logged, and how affected parties receive corrective treatment. Those questions arise from differences between risk identification, control execution, and independent assurance. They provide a more precise conceptual target for the current study without denying the contributions of earlier scholars.

3.3 Digital governance and the missing translation mechanism

Digital governance literature provides tools for explaining rule embedding, monitoring, and feedback. Continuous observation can reduce reliance on infrequent reporting, yet the same infrastructure may produce opacity if its inputs, decision logic, or escalation procedures cannot be interrogated (Yeung, 2018). The crucial analytical point is that more automation is not necessarily more governance. Effective oversight depends on the provenance of rules, evidence quality, defined responsibility, and a functioning possibility of human intervention. These insights expose a translation problem across bodies of literature. Institutional scholarship identifies legitimate authority and organizational controls. Maqasid scholarship clarifies substantive normative objectives. Financial technology scholarship describes technical and organizational change. Regulatory technology research explains monitoring and automation. What remains to be specified is how these components form one accountable cycle in an Islamic financial platform: authorization, implementation, surveillance, escalation, remediation, and learning. This study addresses that design-level gap rather than claiming an exhaustive absence of relevant research.

3.4 Synthesis and boundaries of the contribution

The literature supports four analytical requirements. First, responsibility for Shariah decisions must remain attributable to competent and authorized parties. Second, approved decisions must be expressed as auditable operational specifications. Third, technical controls and human monitoring must generate usable evidence of deviations. Fourth, remedial decisions and governance learning must feed back into platform configurations and oversight records. These requirements collectively motivate the framework developed below. The contribution is deliberately bounded. It does not propose a new Shariah ruling, introduce a universal regulatory standard, or establish the causal effects of automation on user trust. It presents a theory-informed design that can be assessed against actual Saudi platform processes and applicable legal obligations. The same distinction guides the methodology and interpretation of the proposed indicators.

4. Research Methodology

4.1 Conceptual design and unit of analysis

This article uses a conceptual theory-building design. Its unit of analysis is the governance system of a digital platform offering financial services presented as Shariah-compliant, including the relationships among licensed entities, Shariah decision makers, management, technical operators, and users. The paper does not use interviews, surveys, administrative transaction records, or experimental observations. Its conclusions are conceptual propositions derived from scholarship and publicly available institutional documents, not measured findings about particular firms. Conceptual development is appropriate because the question concerns the architecture and logic of a proposed governance arrangement rather than the estimation of a population parameter. The study analyzes

how established institutional and normative concepts may be linked through operational controls. It does not claim to be a systematic literature review, does not report an exhaustive search, and does not imply that included publications form a statistically representative sample of scholarship.

4.2 Source selection and analytical procedure

The conceptual corpus comprises foundational institutional theory; scholarship on Maqasid al-Shariah and Islamic financial governance; research on financial technology, algorithmic governance, and regulatory innovation; contemporary conceptual work on Islamic financial technology; and public Saudi regulatory materials. Sources were chosen purposively for their relevance to one of three analytical questions: who has legitimate authority, what substantive obligations are to be protected, and how can those obligations remain observable during digital execution? Official Saudi materials were used to establish the jurisdictional scope of examples, not to infer obligations beyond their express coverage. The analysis followed five linked operations. First, it distinguished formal oversight from operational execution and identified possible points at which the two could diverge. Second, it assigned governance concerns to institutional, normative, technological, operational, or outcome categories. Third, it examined dependencies among categories to avoid treating control layers as independent silos. Fourth, it specified forward flows of authorization and backward flows of evidence, correction, and reassessment. Fifth, it derived candidate indicators aligned with each layer, explicitly separating design proposals from validated measurement instruments.

The resulting framework was assessed conceptually against three coherence tests. The authority test asks whether a technical control can be traced to an identifiable Shariah or regulatory source. The operational test asks whether the framework can describe a complete path from a decision to transaction execution and exception handling. The normative test asks whether proposed control outcomes can be evaluated in relation to fairness, accountability, and protection without replacing binding Shariah requirements with generalized ethical preferences. Passing these conceptual tests establishes internal design coherence only; it does not demonstrate real-world effectiveness.

4.3 Propositions and limits of validation

Four propositions were formulated as implications of the framework rather than tested hypotheses. They concern traceable authorization, change control, corrective feedback, and outcome assessment. Their directional logic allows later research to investigate whether actual controls correspond to the proposed mechanisms, how implementation varies across licenses and business models, and whether changes in controls relate to measured governance outcomes. No statistical tests, effect sizes, or estimates are reported or implied in the present study. The design is context-sensitive rather than jurisdictionally prescriptive. References to the Saudi Central Bank and Capital Market Authority identify parts of the environment within which a platform may operate. Whether a particular platform is subject to any specific instrument depends on its license, service, legal form, and supervisory classification. This scope restriction is incorporated in the first layer of the framework.

5. Operational Shariah Governance Framework

5.1 Design logic and the meaning of operationalization

The proposed Operational Shariah Governance Framework distinguishes approval of a product from assurance of its continued operation. Ex ante review determines whether a contemplated structure meets the relevant Shariah requirements. Operational governance asks whether later design decisions,

system behavior, disclosures, transaction ordering, amendments, and exceptions remain consistent with that approval. The distinction does not displace ordinary review and audit. Instead, it specifies the controls and evidence needed to connect reviews to day-to-day execution. Four layers perform enabling functions: institutional governance, Shariah governance, technology and regulatory technology, and operational compliance. A fifth layer records governance outcomes and legitimacy. Treating outcomes as the consequence and feedback source of the other four resolves a conceptual ambiguity that would arise if outcome measures were presented as another control mechanism. The architecture is circular in its learning dynamics but ordered in responsibility: authority flows toward implementation, whereas operational information flows toward review and governance decisions.

Governance responsibility may be distributed across licensed firms, outsourced software suppliers, Shariah committees, risk functions, auditors, and regulators. Distribution should not create ambiguity over accountability. The framework therefore requires identification of the responsible owner of each control, the document or decision authorizing it, the process in which it is enforced, and the route by which failures are escalated. A platform could implement these requirements through different technologies depending on its scale and risk profile.

5.2 The five-layer architecture

Layer 1: Institutional governance. This layer identifies the regulated activity, applicable supervisory framework, board and management responsibilities, outsourcing arrangements, and risk ownership. Its outputs include a governance responsibility map, an applicable-obligations register, and approval pathways for material platform changes. The central objective is not to add another committee but to establish who is responsible for converting requirements into operational instructions, approving exceptions, and overseeing corrective action. The Saudi banking framework illustrates the importance of clearly allocated responsibilities where that instrument applies (Saudi Central Bank, 2020). Layer 2: Shariah governance. This layer defines the competent source of Shariah determinations, the record of approved contractual structures, review and escalation mandates, and procedures for reassessing changes. It translates authorized decisions into requirements sufficiently specific to be implemented and tested. Examples include transaction-sequence conditions, required customer disclosures, prohibited fee configurations, and rules for handling a failed or reversed execution step. The layer preserves human scholarly judgment over interpretation while permitting technical specialists to advise on what a software workflow actually does.

Layer 3: Technology and regulatory technology. This layer converts approved requirements into version-controlled technical specifications, configuration tests, monitoring rules, alerts, and audit trails. It should connect every material control to its business process and authorizing decision. Release approval, separation of duties, privileged-access restrictions, change logs, and exception detection are possible mechanisms. Automated checks may identify predefined deviations, but a successful system test is not itself a Shariah opinion. Human governance must remain able to inspect the control logic, question the sufficiency of the evidence, and intervene when a material issue occurs. Layer 4: Operational compliance. This layer covers actual customer and transaction journeys: onboarding, eligibility, disclosure, contracting, settlement, servicing, complaints, reversal, and post-transaction review as applicable to the product. It tests whether approved controls work under routine and exceptional conditions. When a deviation occurs, the process records its severity, affected transactions, responsible owner, interim protection, remedy, and closure decision. Customers should not bear avoidable harm simply because a software error was detected after the system completed the transaction. The operational record also enables periodic independent review.

Layer 5: Governance outcomes and legitimacy. This layer evaluates whether the preceding controls produce credible evidence of conformity and fair treatment. Proposed dimensions include Shariah exception incidence, timely correction, transparency of disclosures, auditability, stakeholder confidence, and reasoned alignment with Maqasid objectives. These dimensions remain analytically distinct: high customer satisfaction cannot offset a material Shariah breach, and an absence of detected incidents does not necessarily prove the absence of incidents. Outcome evidence must therefore be interpreted alongside monitoring coverage, risk exposure, and the reliability of reporting. The architecture is shown in Figure 1. The direction of the downward flow represents authorization, specification, and execution. The upward path represents evidence, incident escalation, independent review, and corrective learning. The outcomes layer informs both routes by revealing whether a technically compliant process is substantively protective and institutionally credible.



Figure 1. Operational Shariah Governance Framework for Islamic financial technology platforms.

5.3 Governance mechanisms across the service lifecycle

The framework's first mechanism is authorization traceability. Every material product requirement should connect an authoritative decision to an operational specification and a documented owner. For example, an approved financing product may require a particular transaction sequence. When developers implement that sequence, the test specification must identify the relevant approval and demonstrate the circumstances in which the sequence is followed or prevented. A disconnected policy document would not meet this standard because reviewers could not establish whether the approved arrangement governs actual execution. The second mechanism is controlled adaptation. Digital services change through product releases, application programming interfaces, external service integrations, commercial campaigns, and adjustments to pricing or eligibility logic. The governance

question is whether a proposed change affects a previously approved Shariah assumption. Materiality screening should occur before deployment; changes with a Shariah effect should enter the authorized review route. The framework does not require every minor interface modification to undergo full scholarly reconsideration, but it does require a defensible record of why the change did or did not need it.

The third mechanism is continuous exception intelligence. Technical logs and transaction data should identify deviations from defined rules, while human review determines their relevance and response. An alert that is technically accurate but too vague to identify affected customers is of limited governance value. Conversely, a highly detailed system that lacks accountable remediation may collect extensive data without improving protection. Effectiveness depends on both detection and closure, measured against the materiality and volume of relevant activity. The fourth mechanism is corrective feedback. A Shariah incident should not end with a report that is filed and forgotten. Responsible governance functions should determine the scope of affected operations, authorize remediation, assess whether the original control failed by design or implementation, and verify that the corrective release resolved the root cause. This sequence links the institutional demand for accountability to the Maqasid concern for actual effects on people and wealth.

These mechanisms can be illustrated through a hypothetical financing workflow. A committee approves a defined product structure. Governance officers identify transaction conditions and disclosures; developers implement them as tested rules; release controls verify the relevant sequence; monitoring detects an exceptional execution path; compliance staff investigate; authorized Shariah personnel determine the treatment of the exception; and management verifies remedy and prevention. The illustration demonstrates design logic only and is not a reported case from a Saudi institution.

5.4 Conceptual propositions

Proposition 1 states that greater traceability between authoritative Shariah decisions and platform-level control specifications should reduce the likelihood of unrecognized divergence between approved structures and executed workflows, subject to the quality of the underlying decisions and technical implementation. The relevant mechanism is transparency of responsibility and reduced ambiguity across organizational boundaries. Proposition 2 states that Shariah-sensitive change screening before platform deployment should improve the consistency of operational compliance over successive software releases. This proposition is conditional on competent review, reliable software inventory, and management support. It is not a claim that change-control procedures already produce such results in Saudi platforms.

Proposition 3 states that feedback systems linking exception detection to accountable remediation should improve the timeliness and completeness of responses to operational Shariah incidents relative to arrangements relying solely on retrospective review. This proposition requires empirical comparison because faster alerts might coexist with poor decision quality or incomplete remediation. Proposition 4 states that governance assessment combining formal compliance, operational evidence, and Maqasid-oriented outcomes should offer a more informative evaluation of platform legitimacy than assessment based exclusively on organizational structures or approval certificates. The proposition does not imply that these dimensions can be reduced to a single valid universal score without substantial measurement work.

5.5 Candidate indicators and measurement considerations

Table 1 translates the five layers into ten candidate indicators retained from the original framework. Their definitions are made more explicit so that future researchers can determine the relevant numerator, denominator, timing, evidence source, or assessment rubric. These are candidate operational definitions, not validated scales and not regulatory thresholds. A low incident count, for example, is only interpretable when monitoring coverage and reporting sensitivity are known.

Table 1. Candidate governance indicators and proposed evidence sources

Governance layer	Candidate indicator	Proposed specification and evidence
Institutional	Regulatory compliance rate	Applicable obligations met / applicable obligations assessed; regulatory obligations register and compliance testing.
Institutional	Governance reporting quality	Completeness and timeliness against applicable reporting duties; approved disclosures and reporting records.
Shariah	Shariah noncompliance incidents	Count and severity of confirmed incidents by exposure and period; adjudicated incident register.
Shariah	Shariah review frequency	Completed risk-relevant reviews against approved review schedule; committee and assurance records.
Technology and regulatory technology	Automated compliance coverage	Relevant transactions or workflow steps monitored / total eligible steps; coverage map and system logs.
Technology and regulatory technology	Exception detection accuracy	Verified alerts relative to reviewed alerts and known exceptions; sampled alert testing.
Operational compliance	Compliance resolution time	Elapsed time from identification to authorized closure, reported by incident severity; case records.
Operational compliance	Operational control effectiveness	Successful control tests / tests executed, with failure criticality; approved tests and release evidence.
Governance outcomes	Stakeholder trust level	Validated survey measure of defined user group; respondent instrument and sampling record.
Governance outcomes	Maqasid alignment assessment	Documented assessment against justified protection, fairness, and disclosure criteria; review rubric.

Note. These are proposed conceptual indicators, not empirically validated measures or mandatory regulatory thresholds. Measurement must preserve both legal and operational specificity. Regulatory compliance rates require an obligations register limited to provisions actually applicable to the platform. Shariah violations require severity classifications approved by competent governance authorities. Stakeholder trust needs a suitable instrument and defined respondent population, while Maqasid alignment needs a reasoned rubric that does not override authoritative transactional requirements. Baselines, thresholds, sampling frames, and inter-rater reliability should be established and tested in a later empirical phase rather than asserted here. The framework can be implemented proportionately. A small platform may use carefully controlled approvals, structured logs, and periodic reconciliations, whereas a high-volume service may justify continuous automated controls and exception dashboards. The essential features are traceability, accountability, reliable evidence, and the possibility of intervention. Technical sophistication alone is not a proxy for governance adequacy.

6. Saudi Arabian Institutional Context

6.1 Differentiated supervisory responsibilities

Saudi financial technology is not a single regulatory category. The appropriate supervisory framework varies with whether a platform provides banking-related activities, payment or financing services, securities activities, or other regulated services. This distinction affects the legality of operations, consumer-protection duties, and how Shariah oversight is organized. As a result, the proposed framework begins with an activity-by-activity regulatory mapping rather than imposing a bank-specific Shariah committee architecture on every platform. For local banks conducting Islamic banking, the Saudi Central Bank's 2020 framework expressly addresses the board, executive management, Shariah committee, and relevant control functions (Saudi Central Bank, 2020). The complementary Shariah-compliant banking risk management framework strengthens attention to risks specific to such activities (Saudi Central Bank, 2022). The 2024 disclosure requirements further establish minimum Shariah governance disclosures for banks within their defined scope (Saudi Central Bank, 2024). These instruments should inform platform controls when they are legally applicable, without being generalized to every nonbank intermediary.

Securities-related platforms require a separate analysis. The Capital Market Authority's move in 2025 to permit debt-instrument crowdfunding under an arranging license illustrates that authorization routes can evolve as financial business models mature (Capital Market Authority, 2025). A platform's Shariah governance design must therefore reflect both its actual business process and the applicable securities framework. The proposed model does not present itself as an official rule issued by either supervisory authority.

6.2 Institutional fit and a practical control map

A Saudi application should document the licensed entity and service, relevant regulatory texts, contractual structure, Shariah approval authority, technical provider responsibilities, consumer disclosures, incident escalation, and reporting lines. A single platform may use external infrastructure for identity verification, payment execution, or record storage. Outsourcing does not eliminate the need to determine who can demonstrate that an approved transaction rule was followed and who will act if outsourced processes fail. The proposed model supports a differentiated approach to control intensity. High-risk changes affecting contract sequence, ownership transfer, pricing, penalties, or product disclosures warrant focused Shariah review and release assurance. Routine modifications without a material Shariah effect may follow documented streamlined controls. All materiality decisions should remain reviewable. This approach avoids requiring manual sign-off for every software event while ensuring that risk-based screening does not become an excuse to bypass competent oversight.

The broader policy significance lies in connecting established governance authorities to auditable digital execution. Such a connection is compatible with innovation because it clarifies what may be automated, which decisions remain reserved to human experts, and how real customer effects inform later design. Its practical sufficiency, however, must be evaluated against actual platform operations and the applicable Saudi legal instruments rather than inferred from conceptual plausibility alone.

7. Discussion

7.1 Theoretical contribution: from governance structures to governance enactment

The framework shifts the explanatory focus from the existence of Shariah governance institutions to the enactment of authorized requirements in a digital service. Institutional theory suggests that formal structures may become separated from organizational practice (Meyer & Rowan, 1977). Operational Shariah governance supplies an explicit mechanism for narrowing this separation: each material decision is linked to a control owner, testable specification, monitored process, and reviewable remedial record. The theoretical contribution is therefore not a rejection of institution-centered governance but an extension of its unit of analysis to the full lifecycle of platform execution. The framework also clarifies the respective roles of institutional theory and Maqasid al-Shariah. Institutional theory explains the sources and organizational conditions of legitimate governance; Maqasid reasoning introduces standards for assessing the substance and effects of financial conduct (Auda, 2008). Neither theory alone specifies how to monitor an automated customer journey. Their integration becomes useful when technological control design is treated as the practical bridge between authority and user experience. This is an explanatory synthesis whose empirical reach remains open to testing.

The five layers represent different analytical functions rather than five equivalent decision-making bodies. Institutional governance establishes authority and legal scope; Shariah governance supplies normative determinations; technology enables systematic enforcement and observation; operational compliance manages actual execution and incidents; outcomes and legitimacy capture evidence of performance and its consequences. The fifth layer is principally evaluative. Its feedback role avoids the logical circularity of assuming that good governance outcomes exist merely because governance structures are present.

7.2 Relationship to contemporary Islamic financial technology frameworks

A central issue for originality is the relationship between the present architecture and existing conceptual proposals. Mohd Najib et al. (2026) explicitly connect Islamic financial technology innovation, Shariah and technology risks, risk-based governance processes, Maqasid principles, and sustainable outcomes. This contribution makes clear that the general integration of Islamic financial technology and Shariah governance is not unique. The present framework makes a narrower claim: it distinguishes governance authority from technical execution, specifies controlled transmission between them, and introduces incident-to-remediation loops with candidate process indicators. This emphasis has a practical implication for research design. Studies that measure only the existence of a committee or an adoption of a policy may miss whether the committee's decisions are implemented in transactional code. Equally, studies that count automated alerts without examining their provenance may miss whether alerts correspond to authorized Shariah requirements. Future empirical research should therefore collect evidence at multiple levels, including governance decisions, release histories, operational logs, exception records, and suitable stakeholder measures. Such a design could test whether the proposed translation mechanism adds explanatory value beyond existing governance characteristics.

7.3 Practical implications for platform operators and assurance functions

For platform operators, the framework supplies a structured means of identifying controls at points where governance and technical activity meet. Product teams can record the Shariah assumptions embedded in a service; developers can maintain tests reflecting those assumptions; compliance teams

can assess deviations; and authorized Shariah personnel can decide whether proposed changes or incidents require reinterpretation or remediation. The value lies in making responsibilities and evidentiary paths explicit rather than multiplying signatures or dashboards. For independent assurance, the model suggests a shift in audit questions. Instead of asking only whether a Shariah opinion exists, a reviewer can select a material product requirement and trace it to the current software specification, release authorization, sample transaction evidence, monitoring rule, and exception-treatment record. Conversely, an operational incident can be traced backward to the approved rule and the decision maker responsible for its interpretation. This bidirectional testing could disclose control weaknesses that would remain invisible if organizational policies were assessed separately from technological operations.

For Shariah governance specialists, the framework emphasizes structured collaboration with technical and risk personnel. A juristic decision may be unambiguous in legal language but still require translation into system states, process order, data fields, and failure conditions. That translation should be documented and reviewed by the relevant expertise rather than presumed correct. The institution should retain responsibility for deciding whether a technical deviation is a material Shariah breach and what corrective treatment is warranted.

7.4 Regulatory and Maqasid-oriented implications

Regulators and standard setters may find value in clearer evidence of the relationship between formal governance obligations and platform operations. Such evidence can support proportionate supervisory dialogue, although the proposed framework is not a replacement for an applicable regulatory instrument. The Saudi example especially shows why an institution must identify the actual activity and governing rule before assigning Shariah or technology control responsibilities. The framework's relevance to nonbank platforms remains a matter of adaptation, not presumed automatic legal coverage. A Maqasid-oriented perspective expands evaluation beyond organizational compliance reports. A platform may be transparent in its annual reporting but opaque in the consumer journey, or technically efficient yet ineffective in resolving disputes. The normative framework therefore calls for evidence about meaningful disclosure, fair handling of exceptional transactions, and the ability to prevent or correct harm. These considerations must be evaluated through appropriately justified measures rather than asserted merely because a platform operates under an Islamic label.

7.5 Research agenda and tests of the framework

Empirical validation should begin with carefully selected case studies across different Saudi financial technology activities. Process tracing could compare a Shariah approval with later system releases and transaction evidence. Interviews with Shariah officers, developers, management, and auditors could clarify where authorization is translated accurately or lost. Transaction-level audits could establish how often predefined deviations occur and how quickly they are investigated and remedied. Such research would directly assess the mechanisms proposed here rather than treating the entire framework as a single unobserved construct. A subsequent quantitative phase could distinguish enabling controls from governance outcomes. For instance, release-screening coverage and alert completeness could be independent explanatory measures, while resolution time or repeat incidents could be outcomes. Trust measures would require appropriately designed respondent instruments and precautions against common-method bias. Comparisons across firms would need to control for service type, platform size, transaction volume, outsourcing dependence, and relevant supervisory regime. The present paper proposes this logic but has not collected the data required to test it.

8. Limitations and Future Research

The principal limitation is the study's conceptual design. The proposed mechanisms and indicators have not been validated through Saudi platform cases, expert consensus, transaction samples, or measurement testing. Accordingly, the article cannot establish the prevalence of governance failures, estimate the effectiveness of regulatory technology, or infer that implementation will increase stakeholder trust. These are researchable propositions, not reported effects. A second limitation concerns scope. Public regulatory documents establish the contours of selected banking and securities frameworks, but the rules applicable to an individual platform depend on its authorization and activity. The analysis does not constitute a legal opinion for every Saudi financial technology business model. Moreover, the candidate indicators may require different denominators, data-access safeguards, and benchmarks across platforms.

Future studies should validate the layer boundaries and causal pathways through expert review, multi-case process tracing, and direct evaluation of control artifacts. Measurement studies should examine indicator reliability, incident classification, and the relationship between monitoring coverage and apparent noncompliance rates. Longitudinal designs could determine whether stronger change governance predicts fewer repeat incidents following product releases. Comparative research may test transferability beyond Saudi Arabia without assuming that other jurisdictions share the same regulatory allocation.

9. Conclusion

This study develops an Operational Shariah Governance Framework for Islamic financial technology platforms in Saudi Arabia. Its starting point is the distinction between Shariah approval and the continuing execution of an approved financial service. Drawing on institutional theory, Maqasid al-Shariah, established Shariah governance principles, and digital governance scholarship, the article specifies how institutional authority can be connected to technology-enabled controls, transaction-level assurance, and responsive corrective action. The framework comprises four enabling layers—institutional governance, Shariah governance, technology and regulatory technology, and operational compliance—and a fifth evaluative layer concerned with governance outcomes and legitimacy. Its distinctive mechanisms are traceable authorization, Shariah-sensitive change control, operational exception intelligence, and corrective feedback. Ten candidate indicators provide a preliminary basis for examining whether these mechanisms exist and function as intended. Neither the indicators nor the framework have yet been tested empirically.

The Saudi application highlights the importance of distinguishing the requirements applicable to banks from those governing other regulated platform activities. Rather than presuming a regulatory vacuum, the framework offers a way to connect existing responsibilities and normative commitments to the realities of software-mediated financial transactions. Its ultimate contribution is a testable account of how Shariah governance may be enacted throughout a digital service lifecycle. Future field studies should examine whether the proposed connections improve control reliability, customer protection, and the credibility of Shariah assurance.

References

- Auda, J. (2008). Maqasid al-Shariah as philosophy of Islamic law: A systems approach. International Institute of Islamic Thought. <https://doi.org/10.2307/j.ctvkc67tg>
- Capital Market Authority. (2025, September 8). The CMA allows crowdfunding of debt instruments through capital market institutions licensed for “arranging” activities. https://cma.gov.sa/en/MediaCenter/NEWS/Pages/CMA_N_3862.aspx
- DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, 48(2), 147–160. <https://doi.org/10.2307/2095101>
- Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services. *Journal of Management Information Systems*, 35(1), 220–265. <https://doi.org/10.1080/07421222.2018.1440766>
- Grais, W., & Pellegrini, M. (2006). Corporate governance and Shariah compliance in institutions offering Islamic financial services (Policy Research Working Paper No. 4054). World Bank. <https://documents.worldbank.org/en/publication/documents-reports/documentdetail/675821468141267256>
- Hasan, Z. (2011). A survey on Shari’ah governance practices in Malaysia, GCC countries and the UK: Critical appraisal. *International Journal of Islamic and Middle Eastern Finance and Management*, 4(1), 30–51. <https://doi.org/10.1108/17538391111122195>
- Hassan, M. K., Rabbani, M. R., & Ali, M. A. M. (2020). Challenges for the Islamic finance and banking in post COVID era and the role of fintech. *Journal of Economic Cooperation and Development*, 41(3), 93–116. <https://journal.sesric.org/Article/Detail/ART20062603>
- Islamic Financial Services Board. (2009). Guiding principles on Shari’ah governance systems for institutions offering Islamic financial services (IFSB-10). https://www.ifsb.org/wp-content/uploads/2023/10/IFSB-10-December-2009_En.pdf
- Lee, I., & Shin, Y. J. (2018). Fintech: Ecosystem, business models, investment decisions, and challenges. *Business Horizons*, 61(1), 35–46. <https://doi.org/10.1016/j.bushor.2017.09.003>
- Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. *American Journal of Sociology*, 83(2), 340–363. <https://doi.org/10.1086/226550>
- Mohd Najib, N. W., Basarud-din, S. K., Abdullah, N. K., & Muhamad, F. N. (2026). Islamic fintech and Shariah governance: A conceptual framework. *International Journal of Research and Innovation in Social Science*, 10(6), 84–96. <https://doi.org/10.47772/IJRISS.2026.100600008>
- Mollah, S., Hassan, M. K., Al Farooque, O., & Mobarek, A. (2017). The governance, risk-taking, and performance of Islamic banks. *Journal of Financial Services Research*, 51(2), 195–219. <https://doi.org/10.1007/s10693-016-0245-2>
- Nomran, N. M., & Haron, R. (2020). A systematic literature review on Shari’ah governance mechanism and firm performance in Islamic banking. *Islamic Economic Studies*, 27(2), 91–123. <https://doi.org/10.1108/IES-06-2019-0013>
- Saudi Central Bank. (2020). Shariah governance framework for local banks operating in Saudi Arabia. <https://rulebook.sama.gov.sa/en/entiresection/2274>
- Saudi Central Bank. (2022). Risk management framework for Shari’ah compliant banking. <https://www.rulebook.sama.gov.sa/en/risk-management-framework-shari%E2%80%99ah-compliant-banking>

- Saudi Central Bank. (2024). Shari'ah governance related disclosure requirements for the banks conducting Shari'ah compliant banking. <https://www.rulebook.sama.gov.sa/en/shari%CA%BCah-governance-related-disclosure-requirements-banks-conducting-shari%CA%BCah-compliant-banking>
- Scott, W. R. (2013). *Institutions and organizations: Ideas, interests, and identities* (4th ed.). SAGE Publications.
- Yeung, K. (2018). Algorithmic regulation: A critical interrogation. *Regulation & Governance*, 12(4), 505–523. <https://doi.org/10.1111/rego.12158>
- Zetsche, D. A., Buckley, R. P., Barberis, J. N., & Arner, D. W. (2017). Regulating a revolution: From regulatory sandboxes to smart regulation. *Fordham Journal of Corporate & Financial Law*, 23(1), 31–103. <https://ir.lawnet.fordham.edu/jcfl/vol23/iss1/2/>