

Financial Risk Governance in Saudi Banking and Fintech Subsidiaries: An Integrated Audit and Compliance Framework for Sustainable Financing

Mohammad Ahsan

Published October 2026

Abstract

Purpose: This review investigates how Saudi banks can govern financial risks arising within affiliated fintech entities while maintaining credit discipline, regulatory compliance and credible sustainable financing. It distinguishes ownership oversight from operational assurance and asks where controls should remain common across a group and where subsidiary-specific arrangements are necessary.

Design/methodology: A structured integrative review synthesises scholarship published between 2020 and 2025 on bank stability, fintech regulation, internal audit, technology risk and sustainability. Contributions from Saudi Arabia and the Gulf are interpreted alongside transferable international findings; no interviews, survey responses or new bank-level observations are claimed.

Findings: Evidence indicates that fintech benefits depend on regulatory capacity, risk culture and control design. The proposed framework links group risk appetite, subsidiary accountability, independent audit testing, transaction-level compliance evidence and financing-outcome review.

Originality/value: It converts fragmented debates into an implementable assurance architecture with explicit escalation rights, measurable indicators and safeguards against overstating sustainability results. Its propositions remain subject to institutional testing.

Keywords: Saudi Arabia; fintech subsidiaries; financial risk governance; internal audit; regulatory compliance; sustainable financing; operational resilience

1 Introduction

Saudi Arabia's financial transformation combines an established banking system with a growing ecosystem of technology-enabled payment, lending and investment services. A bank may own a fintech subsidiary, participate in a joint venture or rely on an external platform to originate transactions and serve customers. These arrangements extend distribution and product reach while creating supervisory boundaries that are less visible than the customer interface. A subsidiary's rapid onboarding process can increase credit exposure, alter funding demands or introduce conduct risks whose consequences ultimately return to the wider banking group. The essential governance question is therefore not whether innovation should proceed, but how financial accountability should follow services across organisational boundaries [2–4].

International evidence does not justify a presumption that fintech automatically makes banks safer. Research across Gulf banking systems associates greater fintech adoption with lower stability on average, but reports meaningful variation by capitalisation, ownership and institutional setting [2]. Other cross-country studies find that the effects of technological change depend on market conditions and regulatory arrangements [16]. These divergent findings imply that a Saudi bank

cannot assess subsidiary risk solely from digital adoption rates, customer growth or platform availability. Exposure limits, decision rights, recovery capacity and the quality of management information must also be evaluated. The same distinction matters when digital lending is promoted as support for economic diversification.

Sustainable financing adds a second accountability problem. Its economic meaning concerns credit-worthiness, appropriate maturities, transparent pricing and the ability to fund productive activity without undermining resilience. Its environmental and social meanings require defensible eligibility criteria, reliable outcome data and evidence that funds are used as represented. The Saudi regulatory literature identifies measurement and market-readiness challenges in aligning finance with national sustainability objectives [1]. For banking groups, these challenges intersect with fintech data infrastructures: automated classifications may travel rapidly through APIs while the underlying audit trail remains incomplete. Governance must prevent operational efficiency from being mistaken for verified financing impact.

This review addresses a gap between three established conversations. Banking research examines audit committees, risk culture and stability; fintech research investigates innovation, sandboxes and cyber threats; sustainable-finance studies analyse disclosure quality and financing objectives [3, 8, 10, 13]. Yet comparatively little work specifies how a parent bank should combine these controls when an affiliated fintech originates, services or monitors exposures. A framework that simply replicates the bank's committee chart would be insufficient because software releases, outsourced data processing and automated credit decisions involve different evidence and response times. The contribution here is a functional integration model linking governance authority to transactions, systems and independent assurance.

1.1 Study aim, objectives and research questions

The study aims to develop a theoretically grounded and operationally testable financial risk governance architecture for Saudi banking groups and their fintech subsidiaries, with sustainable financing treated as an outcome requiring proof rather than as a promotional label. Four objectives guide the review: distinguish subsidiary-specific risks from consolidated bank exposures; assess complementary and conflicting roles of governing bodies and assurance functions; identify a proportionate control sequence for credit, operational, compliance and sustainability risks; and specify evidence by which implementation could be evaluated. The study asks who owns residual risk, how exceptions move between legal entities, which records support independent audit conclusions and how financing benefits can be verified without weakening prudential safeguards.

2 Conceptual foundations

Financial risk governance refers to the allocation of decision authority, risk appetite, monitoring obligations and accountability for losses. Compliance management is narrower: it identifies applicable obligations, translates them into procedures and demonstrates adherence. Internal audit provides independent assurance that governance and controls work as intended, rather than operating the controls on management's behalf. These functions overlap in information but should remain distinct in responsibility. A successful control design therefore depends on both separation of duties and rapid exchange of credible evidence. Kunz and Heitz [3] show why a bank's risk culture cannot be reduced to a checklist; formal incentives, practical challenge and managerial behaviour shape whether warning signals reach decision makers.

For subsidiaries, the principal-agent problem is layered. Parent shareholders delegate authority to a bank board, bank management delegates to subsidiary executives and technical teams may depend on service providers outside the group. At each boundary, commercial incentives can diverge from the consolidated appetite for loss. A local subsidiary may prefer rapid expansion because its profitability is assessed separately, whereas the parent bears reputational and liquidity consequences if systems fail. Governance should therefore couple clearly defined delegated limits with consolidated exposure aggregation. Audit evidence needs to travel in the opposite direction: originating systems must allow the parent to reconstruct decisions, exceptions, overrides and ultimately the quality of financing outcomes.

A three-lines arrangement provides a useful starting vocabulary but not a complete organisational blueprint. Business and subsidiary owners operate product controls and accept only risks within delegated parameters. Independent risk and compliance teams establish interpretations, evaluate exceptions and challenge portfolio assumptions. Internal audit evaluates whether the first two layers and their information interfaces operate effectively. The board and its risk and audit committees oversee the whole arrangement. Evidence that audit-committee effectiveness can reduce bank risk-taking and enhance stability supports independent challenge, but committee architecture and institutional context condition outcomes [5–7]. The framework must therefore specify information rights and escalation deadlines, not merely the existence of committees.

2.1 Fintech business models and consolidated exposures

The label fintech conceals important differences among payment facilitators, digital lenders, credit-scoring suppliers and investment platforms. A payment subsidiary may create settlement, fraud and safeguarding exposures; a lending platform can introduce model risk, collections weaknesses and correlated borrower defaults; a digital investment service raises suitability and valuation concerns. Where activities are outsourced, concentration risk may accumulate at a cloud host or data intermediary. Such activities cannot be governed through a single generic cybersecurity score. Risk identification should connect product, legal entity, customer segment, provider, cash-flow dependency and regulatory permission. The risk taxonomy must also recognise whether the parent provides explicit guarantees or reputational support despite limited contractual obligations [4, 29].

Bank and fintech risks are not additive in a simple arithmetic sense. A service disruption can prevent loan repayments and create operational losses at the same time that customers withdraw funds, raising liquidity requirements. Data corruption may impair underwriting models and cause inaccurate regulatory returns. Berger and colleagues [19] show that operational losses have wider financial-stability implications than an exclusively firm-specific interpretation suggests. Eisenbach and colleagues [20] identify interconnected payments and common providers as channels through which cyber incidents can propagate. In the Saudi context these insights support scenario testing that follows service failure through financial accounts, subsidiaries and counterparties, rather than stopping at the affected application.

3 Review methodology

This article adopts a structured integrative literature review because the research question spans banking governance, financial technology, internal audit, regulatory administration and sustainable finance. Heterogeneous conceptual, quantitative and policy studies cannot be meaningfully pooled into a single effect estimate. The unit of analysis is an argument or finding relevant to governance

design, not a constructed sample of Saudi subsidiaries. Scholarly and institutional sources dated 2020–2025 were identified through targeted searches of publication records and DOI-linked article pages using combinations of bank risk, fintech stability, audit committee, operational risk, regulatory sandbox, compliance, ESG and Saudi Arabia. The Saudi sustainable-finance study helped identify the local contextual framing [1].

Selection prioritised sources addressing at least one of four domains: bank risk and prudential stability; assurance or board accountability; fintech operational and compliance exposures; or measurable sustainability-related finance. Gulf and Saudi evidence received higher contextual weight, while international evidence was retained where the causal mechanism appeared transferable. Sources lacking identifiable publication information or a consistent link to the research question were excluded. For each retained source, the synthesis recorded its jurisdiction, method, governance mechanism, reported direction of evidence and main applicability limitation. The 30-item bibliography is an analytic set rather than a claim that all relevant papers were exhaustively captured.

Thematic comparison proceeded in three stages. First, empirical findings were separated from recommendations, preventing proposed mechanisms from being described as demonstrated effects. Second, convergent and contradictory conclusions were compared across institutional conditions; in particular, fintech's influence on stability was not treated as uniform. Third, common control requirements were translated into design propositions concerning ownership, traceability, assurance independence and financing integrity. No regression coefficients, interview quotations or counts of screened records are presented because the review did not generate those observations. It is not a quantitative meta-analysis, and its limitations include publication selection, contextual transferability and a lack of subsidiary-level implementation tests.

4 Evidence synthesis: bank risk, governance and audit

Bank stability is influenced by governance arrangements that operate well before a crisis appears in financial statements. The literature maps relationships among risk-taking, regulation and profitability, but cautions against reducing governance to one indicator [8]. Cross-country fintech research likewise suggests that technological expansion may raise or lower fragility depending on institutional characteristics [9, 16]. These findings imply that the board should define a risk appetite that combines solvency and liquidity measures with operational indicators such as system availability, exception backlog and high-risk customer exposure. A subsidiary dashboard consisting only of revenue, transaction volume and acquisition cost would conceal meaningful group risks.

Internal audit's contribution is strongest where it investigates the actual transmission of risk through procedures and information systems. Nguyen [5] links effective audit committees to bank efficiency and lower risk-taking, while separate evidence connects committee structure and institutional quality with stability [26]. These studies are not direct evaluations of Saudi fintech subsidiaries, and committee effects cannot simply be imported as universal prescriptions. The practical inference is more modest: independent oversight should challenge management's claims using timely and reconstructable evidence. Audit plans ought to test onboarding approvals, credit-limit overrides, customer-fund reconciliations, ledger interfaces, complaints and third-party incident logs, including whether exceptions were resolved within approved tolerances.

Oversight quality also depends on capacity. Ashraf, Choudhary and Jaggi [7] caution that assigning extensive risk responsibilities to audit committees may create monitoring overload. For a fintech portfolio with frequent releases and diverse products, a bank should therefore define which issues

are reviewed by technology and operational-risk specialists, which warrant executive escalation and which demand board-level consideration. Internal audit should report systemic themes, root causes and overdue remedies rather than relay every technical exception. A risk committee may own appetite and emerging exposure; an audit committee should protect the independence and quality of assurance. Clear boundaries reduce both duplication and unmanaged gaps.

Risk culture provides the behavioural mechanism between formal policy and actual decisions. Rapid growth can normalise short-term exceptions when incentive structures favour transaction throughput, while compliance teams are rewarded for speed rather than substantive challenge. Research on management controls stresses the interaction of values, staffing, rewards and actions [3]. In an affiliated fintech, that means monitoring not only the proportion of automated approvals but also the frequency, reason and authorisation of overrides. Boards should require evidence that employees can raise concerns without commercial retaliation. A credible culture indicator is the treatment of previously reported exceptions, not an unverified claim of universal policy awareness.

4.1 Regulatory compliance and subsidiary accountability

Regulatory innovation has a dual purpose: enable experimentation and keep risks within acceptable boundaries. Research on guided regulatory sandboxes argues for active supervisory engagement rather than treating permission to test as a substitute for complete controls [17]. Studies of fintech sandbox activity and investment describe benefits for innovation but also indicate that supervision must evolve with business models [22]. For Saudi banks, the implication is to maintain a licensing and obligation inventory for every subsidiary and outsourced activity. Permission to offer one product should never be presumed to cover an adjacent product, customer class or data-processing arrangement. Compliance interpretations should be periodically refreshed against authoritative local requirements.

The compliance inventory should be connected to each product's transaction lifecycle. Account opening requires identity, customer due-diligence and consent evidence; financing requires suitability, contractual documentation and decision traceability; payments require screening, settlement and safeguarding controls; closure requires retention and complaint handling. Each obligation needs a named control owner, evidence repository, monitoring frequency and breach pathway. Anti-money-laundering research shows both the promise of automated detection and the importance of safeguards against unjustified decisions [21]. A model's high alert volume is not evidence of control effectiveness when investigators cannot distinguish material cases, explain decisions or document proportional responses.

4.2 Technology, cyber and third-party dependence

Fintech dependence changes the speed at which errors can multiply. An incorrectly deployed software rule may affect thousands of customer transactions before traditional reconciliations occur. Saudi consumer research reports material concerns about banking cybersecurity, underlining trust as well as technical protection [18]. Studies of fintech's risk landscape identify a shift from physical crime towards cyber-enabled threats and gaps between rapidly changing technology and supervisory capacity [30]. Accordingly, board reporting should distinguish prevented incidents, undetected exposure and actual customer harm. A system can be available yet unsafe because privileged access, data lineage or model outputs are compromised.

A robust control architecture should place security checkpoints within the change process, not only at annual audit. Privileged identities must be reviewed independently; high-impact model changes should require controlled testing, documented approval and rollback options. Third-party arrangements require exit planning, disaster-recovery exercises and contractual rights to obtain incident evidence. Operational resilience is measured by the organisation's ability to preserve essential services under severe but plausible disruption, including manual fallback where necessary. Financial accounts must also be reconciled after recovery. Without this step, technical restoration might coexist with misstated customer balances, duplicated payments or unrecognised financial losses [19, 20, 25].

5 Sustainable financing as a governed outcome

Sustainable financing should be defined at instrument and portfolio level, with financial viability distinguished from environmental or social claims. For a small-business loan, the bank must establish repayment capacity and affordability irrespective of projected developmental benefits. If the loan is additionally described as green or socially beneficial, measurable eligibility and use-of-proceeds information are needed. Saudi finance scholarship identifies regulatory harmonisation, data standardisation and measurement challenges in developing credible green finance [1]. The proposed framework therefore treats sustainability attributes as additional evidence requirements rather than as offsets against credit weakness. This avoids allowing a favourable classification to dilute underwriting limits or expected-loss discipline.

International banking evidence suggests relationships among sustainability performance, lower risk exposures and improved valuation, but it cannot establish that every labelled financing product is low risk [12, 13]. Gulf research further identifies links between fintech, governance and ESG outcomes, with heterogeneous effects across banking types and ownership forms [14]. This variability makes impact governance essential. A bank should specify what constitutes an eligible sustainable asset, which records substantiate the classification, who checks material changes in use of funds and how inaccurate classifications are corrected. Independent audit can test the consistency of claims with underlying documents without assuming responsibility for originating or marketing the financing product.

Digital tools can support a richer audit trail. Transaction identifiers may connect credit approval, disbursement, vendor invoices and subsequent impact reporting, allowing discrepancies to be traced more quickly. Yet data integration does not guarantee truth: self-reported emissions figures or supplier declarations may be unreliable even when immutably stored. Literature on fintech collaboration and sustainability emphasises organisational choices and governance rather than technological determinism [15, 28]. An appropriate control is thus to distinguish validated performance measures from estimates, disclose uncertainty and maintain the ability to revise a claim. Where impact cannot be demonstrated, reporting should describe intended allocation instead of asserting achieved outcomes.

6 Proposed integrated audit and compliance framework

Figure 1 sets out the proposed functional architecture. A bank-group board establishes risk appetite and the oversight mandate, while each subsidiary retains identified responsibility for its products, customers and control operation. Enterprise risk management aggregates capital, credit, liquidity, operational and conduct exposures and challenges assumptions across legal entities. A common evidence layer links transactions, models, approvals, regulatory obligations and sustainability

classifications. Independent internal audit tests this information and reports assurance gaps to the appropriate governing committee. The architecture is deliberately not a proposal to centralise every decision: local teams must have authority to stop unsafe processes, while group management must be able to restrict an activity that threatens consolidated resilience.

The framework begins with a product-level risk and obligation assessment before customer launch. Each product receives a taxonomy of exposures, a limit structure, scenario tests and a mapped set of laws and policies. Control designs require evidence that both normal and exceptional transactions can be reconstructed. At execution, automated rules block forbidden actions, flag threshold breaches and preserve immutable or appropriately protected event histories. Exception owners provide reasoned dispositions and timed remedies. The group risk function examines cross-subsidiary concentration, while compliance evaluates regulatory treatment and suspicious patterns. Internal audit subsequently samples transactions, re-performs reconciliations and tests whether reported metrics correspond to source records.

Audit independence is particularly important when fintech engineering teams create their own monitoring dashboards. Dashboard accuracy must be verified through direct testing of data lineage and completeness, not assumed from attractive visualisations. Auditors should have read-only access to relevant logs, production change approvals, privileged-access histories and customer complaint records, subject to confidentiality controls. Where data are held by an external provider, contractual inspection rights should be tested before a crisis. Audit observations should distinguish isolated noncompliance from systemic design defects. A recurring reconciliation break, for example, may signal a flawed interface rather than repeated individual negligence and calls for an architectural remedy.

The parent should maintain an auditable chain of delegation. Board-approved appetite translates into subsidiary mandates, portfolio thresholds, product conditions and individual approval privileges. Each override has an identified authoriser, justification and expiry; material departures require immediate consolidation-level escalation. Exceptions should be rated using expected financial severity, customer impact, legal consequences and recoverability. Thresholds need not be identical across products, but the logic for their assignment should be comparable. Thus, a failed high-value settlement is escalated rapidly even when rare, whereas recurring low-value fee errors may trigger a systemic conduct review once their cumulative impact exceeds tolerance.

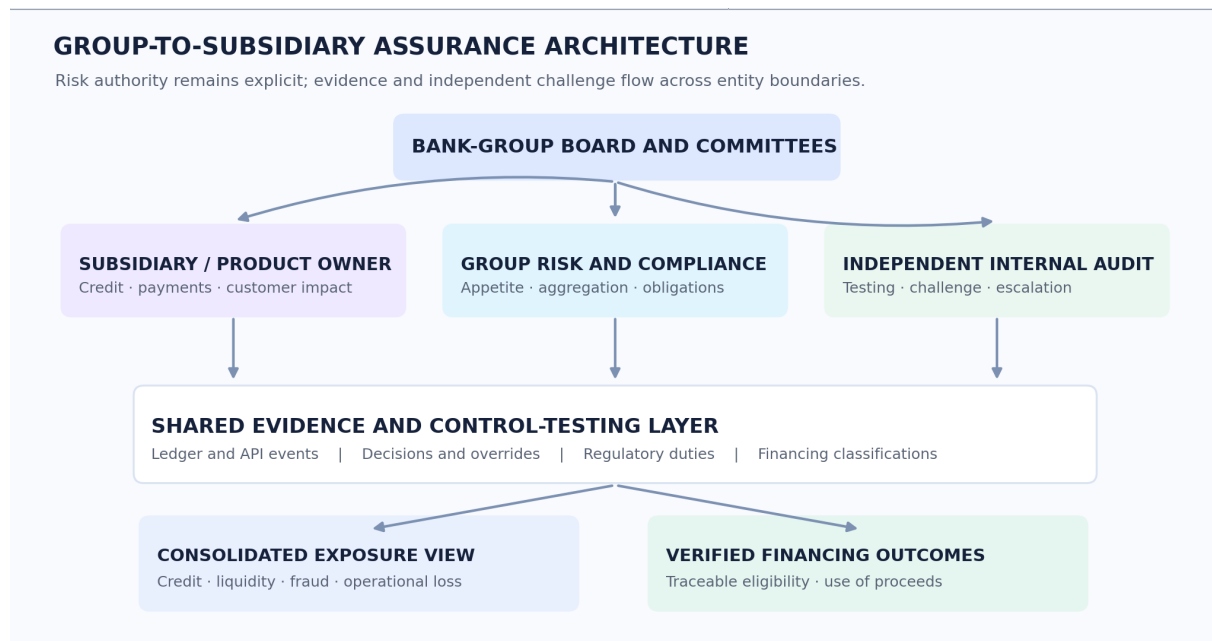


Figure 1. Proposed group-to-subsidary governance and assurance architecture (original conceptual design).

6.1 Control matrix and measurable assurance

Table 1 associates each major exposure with an accountable owner, primary control and independent assurance test. It deliberately separates the entity responsible for operating a control from the party evaluating its design. Credit risk requires periodic back-testing of scorecards and review of forbearance and staging decisions; liquidity risk requires stress scenarios that recognise settlement delays and parent support; operational risk requires service recovery and reconciliation tests; compliance requires traceable customer decisions; sustainability classification requires source-data verification. These controls should be prioritised according to materiality rather than inspected at uniform frequency. Risk appetite should incorporate plausible stress losses, not merely historical incident counts.

An assurance scorecard should combine leading and lagging indicators. Leading measures include unresolved critical vulnerabilities, aged regulatory findings, stale customer due-diligence records, model drift and concentration of cloud or payment-service providers. Lagging measures include confirmed fraud losses, customer remediation costs, rejected regulatory returns, nonperforming financing and verified service outages. A high rate of closed audit recommendations becomes misleading if matters recur in a new form. Consequently, closure evidence should include sustainable corrective action and a follow-up test rather than acceptance of an owner statement. Reported metrics should retain definitions and stable denominators to prevent apparent improvements generated by measurement changes.

Table 1. Exposure ownership, management controls and independent assurance tests.

Exposure	Accountable function	Key preventative/detective controls	Independent assurance test
Credit and model	Lending subsidiary; group credit risk	Approval limits; model drift; staging and override logs	Re-perform approval paths and sampling of overrides
Liquidity and settlement	Group treasury; payment operation	Cash-flow stress; safeguarding reconciliation; settlement alerts	Trace break items and stress assumptions to source

Exposure	Accountable function	Key preventative/detective controls	Independent assurance test
Cyber and outsourcing	Technology risk; provider owner	Identity control; change gates; backup and recovery tests	Inspect privileges, release evidence and recovery drills
Financial crime / conduct	Compliance; product executive	Customer screening; transaction monitoring; complaint escalation	Retest case selection, decisions and complaint closure
Sustainability claims	Financing owner; sustainability office	Eligibility rules; outcome evidence; use-of-funds tracking	Compare labelled exposures with verified underlying records

6.2 Decision cycle and escalation

Figure 2 translates the model into a recurrent assurance cycle. Risk assessment identifies material exposures and regulatory duties; execution produces transaction and system evidence; continuous monitoring compares outcomes with limits; independent challenge tests controls and reported results; correction assigns accountable remedies; and learning changes standards, incentives or product configurations. The cycle also requires explicit stop conditions. Repeated data integrity failures, unauthorised lending logic or unresolved breaches of customer-fund protection should be capable of suspending a product before the next scheduled committee meeting. Escalation is effective only when authority, substitute decision makers and communication channels have been rehearsed in realistic scenarios.

The control cycle must recognise different time horizons. Automated fraud decisions may require action in seconds, liquidity management operates throughout the trading or settlement day, credit reviews may occur monthly and board appetite assessments quarterly. A single reporting cadence cannot cover all of them. Instead, the operating model should require immediate exception triggers and periodic strategic review using consistent definitions. Internal audit has no mandate to become a continuously staffed operations centre; it evaluates the design and reliability of monitoring and may use data analytics to select high-risk samples. This distinction preserves assurance independence while enabling faster management response.

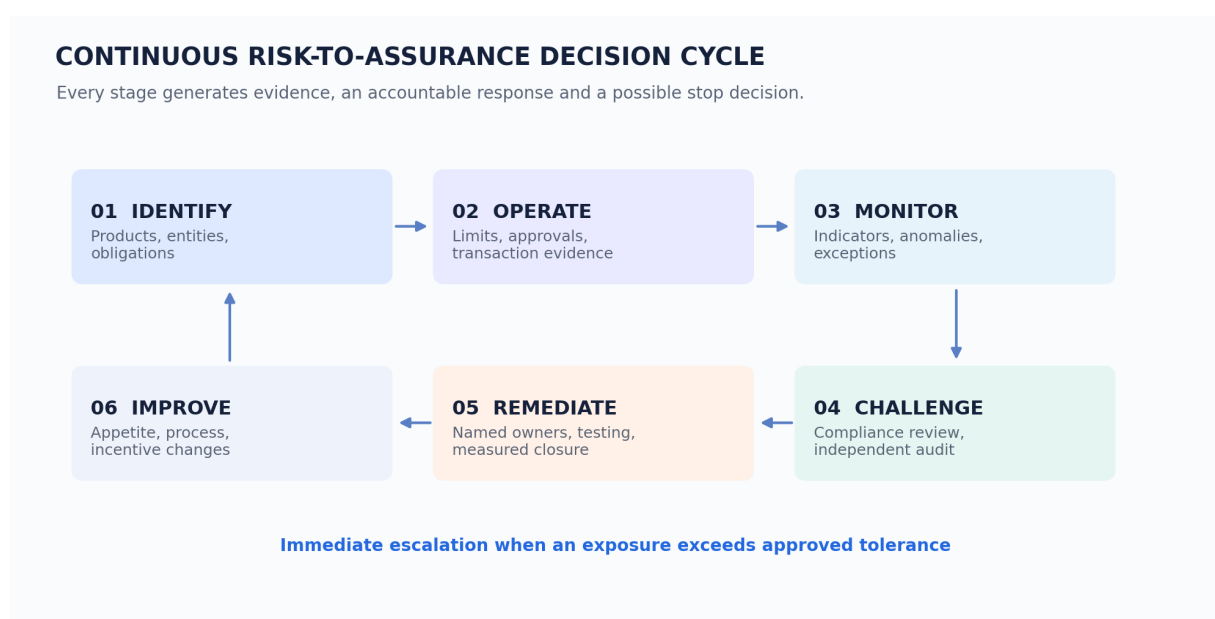


Figure 2. Proposed assurance and escalation cycle (original conceptual design).

7 Critical discussion

The literature resists a simple technology-versus-regulation narrative. Fintech can broaden access and reduce information frictions, yet increase interconnectedness, outsourcing dependence and opportunities for rapid error propagation [4, 10, 11]. Similarly, risk governance can protect financial stability but may impede legitimate innovation if approvals are rigid and duplicated. The proposed answer is proportionality with common minimum controls: product teams retain flexibility over customer experiences, while identity integrity, ledger reconciliation, material risk limits and audit access remain mandatory across entities. It is a method of allocating scarce supervisory attention to activities with the greatest potential to transmit loss.

A second tension concerns consolidated control and subsidiary accountability. Overcentralisation can weaken local knowledge of fraud patterns and customer needs; excessive decentralisation obscures common exposures and inconsistent interpretations. A federated model uses a common taxonomy and reporting standard while retaining specialist judgement near the transaction. However, its effectiveness relies on skilled personnel, reliable information interfaces and governance incentives. Banking evidence shows that the financial implications of fintech vary by institutional setting and bank structure [2, 9, 16]. Accordingly, implementation should be assessed against each institution's asset mix, financing arrangements, provider dependencies and supervisory obligations before the framework is presented as generally effective.

A third tension arises from sustainability claims. Effective lending controls may reject a socially desirable venture whose cash flows cannot support repayment, whereas a financially strong borrower may provide inadequate evidence for green classification. These decisions concern different forms of evidence and should not be compressed into one composite rating. Research on ESG controversies and bank risk supports attention to disclosure integrity [12], while studies of fintech and bank greenwashing suggest that digitalisation can influence information asymmetries without eliminating incentives to misreport [27]. A disciplined bank should therefore record the financial decision, sustainability classification and impact assurance separately. Transparent disagreement is preferable to a polished but untestable composite score.

Technology-enabled controls also create a danger of circular assurance. If a fintech's credit model generates a risk score, its monitoring layer aggregates that score and internal audit relies exclusively on the dashboard, every stage may inherit one data error. Independent assurance should include alternative source records, manual re-performance and model outcome checks. An analogous concern arises when automated anti-money-laundering detection uses poorly understood features: decision efficiency does not excuse discriminatory or unjustified outcomes [21]. Good governance is therefore evidenced by independent routes to challenge technical outputs, sufficient access to raw evidence and a mechanism to suspend models when their limitations become material.

Table 2. Critical evidence synthesis and limits of transferability.

Evidence strand	Synthesis from 2020–2025 studies	Interpretive boundary	Implication for the framework
Fintech and bank stability	Effects differ across capitalisation and institutional context [2, 9, 16]	Associations are not causal Saudi subsidiary tests	Set group risk appetite and study concentration
Audit and governance	Committee design can support stability, but overload matters [5–7]	Evidence spans different jurisdictions	Separate challenge, escalation and operational duties

Evidence strand	Synthesis from 2020–2025 studies	Interpretive boundary	Implication for the framework
Operational resilience	Losses and cyber disruption can propagate [19, 20, 24]	Impact depends on networks and providers	Reconcile post-recovery transactions and stress shared dependencies
Compliance innovation	Sandbox and AI tools help, but safeguards remain necessary [17, 21–23]	Pilot permission is not permanent approval	Map obligations to product controls and evidence
Sustainable finance	ESG associations vary; data and classification require scrutiny [1, 12–15, 27–29]	ESG indicators do not prove individual loan impact	Independent eligibility and use-of-funds checks

8 Practical implementation and research agenda

Implementation should proceed through controlled stages rather than a group-wide policy announcement. Initially the bank should inventory subsidiaries, product permissions, material outsourcing and consolidated risk exposures. It should then map one high-priority product from application to settlement, collections, complaint handling and regulatory reporting. A pilot can test whether exceptions move consistently between subsidiary operations, risk, compliance and audit. The next stage should establish common evidence definitions and group reporting, followed by scenario exercises combining technology incidents with liquidity and customer consequences. Expansion should depend on documented control effectiveness, not merely delivery milestones or the completion of training sessions.

Regulatory engagement should also inform how pilot activities become permanent products. Sandbox evidence concerns constrained tests, not proof that a mature bank-group arrangement is safe at scale [22]. The parent should specify an exit condition for every pilot: data reconciliation must be repeatable, complaints must be reviewable, model monitoring must function under live volumes and supervisory commitments must be mapped to continuing owners. A permission register should distinguish initial testing authorisation from the conditions governing full operation. This makes regulatory learning a controlled component of strategic investment instead of an administrative hurdle completed once.

Future empirical research could compare subsidiary structures with different levels of common control ownership, assess whether independent audit access predicts shorter remediation periods and investigate the financial cost of delayed exception escalation. A mixed-method design could combine board documentation, event-level logs, supervisory correspondence and interviews, subject to permissions and confidentiality. Longitudinal work would be valuable because newly established subsidiaries may exhibit strong launch controls that deteriorate during product expansion. Researchers should distinguish correlation from causation, establish comparable exposure denominators and measure both constrained risk and economically valuable innovation. Such tests would determine whether the proposed framework improves resilience rather than merely increasing governance paperwork.

Institutional capacity can be evaluated without overstating what international studies show. Evidence concerning audit committee structure and bank stability is jurisdiction-dependent and should not be read as an instruction to copy a particular committee size [26]. Guidance on central-bank technology risk likewise emphasises integrated risk ownership, board awareness and response planning, but it does not substitute for a local legal interpretation [24]. A useful governance maturity assessment

would therefore test the strength of escalation, the clarity of delegated authority and the reproducibility of incident evidence in each Saudi entity. These characteristics remain relevant regardless of whether the subsidiary supplies lending, payments or investment technology.

9 Conclusion

Saudi banks and fintech subsidiaries cannot sustain financing growth through technological capability alone. The reviewed evidence identifies an interdependent need for prudent risk-taking, credible compliance interpretation, operational resilience, governance challenge and verifiable sustainability claims. The article proposes a federated assurance framework in which board appetite, subsidiary decision rights, common evidence standards, cross-entity risk aggregation and independent audit work together without erasing local accountability. Its central proposition is that governance quality depends on whether material decisions and exceptions can be traced, challenged and corrected before they transmit loss. The model is conceptual, not validated by new Saudi bank observations. Its value lies in specifying propositions and auditable implementation requirements that subsequent empirical studies can test.

References

- [1] Alhejaili MO. Integrating climate change risks and sustainability goals into Saudi Arabia's financial regulation: pathways to green finance. *Sustainability*. 2024;16:4159. <https://doi.org/10.3390/su16104159>
- [2] Khan HH, Khan S, Ghafoor A. Fintech adoption, the regulatory environment and bank stability: an empirical investigation from GCC economies. *Borsa Istanbul Review*. 2023;23(6):1263–1281. <https://doi.org/10.1016/j.bir.2023.10.010>
- [3] Kunz J, Heitz M. Banks' risk culture and management control systems: a systematic literature review. *Journal of Management Control*. 2021;32:439–493. <https://doi.org/10.1007/s00187-021-00325-4>
- [4] Murinde V, Rizopoulos E, Zachariadis M. The impact of the FinTech revolution on the future of banking: opportunities and risks. *International Review of Financial Analysis*. 2022;81:102103. <https://doi.org/10.1016/j.irfa.2022.102103>
- [5] Nguyen QK. Audit committee effectiveness, bank efficiency and risk-taking: evidence in ASEAN countries. *Cogent Business & Management*. 2022;9:2080622. <https://doi.org/10.1080/23311975.2022.2080622>
- [6] Nguyen QK. Oversight of bank risk-taking by audit committees and Sharia committees: conventional vs Islamic banks. *Heliyon*. 2021;7:e07798. <https://doi.org/10.1016/j.heliyon.2021.e07798>
- [7] Ashraf M, Choudhary P, Jaggi J. Are audit committees overloaded? Evidence from the effect of financial risk management oversight on financial reporting quality. *Management Science*. 2024;70(12):8414–8447. <https://doi.org/10.1287/mnsc.2022.00360>
- [8] Rastogi S, Sharma A, Pinto G, Bhimavarapu VM. A literature review of risk, regulation, and profitability of banks using a scientometric study. *Future Business Journal*. 2022;8:28. <https://doi.org/10.1186/s43093-022-00146-4>
- [9] Safiullah M, Paramati SR. The impact of FinTech firms on bank financial stability. *Electronic Commerce Research*. 2024;24:453–475. <https://doi.org/10.1007/s10660-022-09595-z>
- [10] Liu Y, Abdul Rahman A, Mohd Amin SI, Ja'afar R. Navigating fintech and banking risks: insights from a systematic literature review. *Humanities and Social Sciences Communications*. 2025;12:717. <https://doi.org/10.1057/s41599-025-05055-9>
- [11] Cevik S. The dark side of the moon? Fintech and financial stability. *International Review of Economics*. 2024;71:421–433. <https://doi.org/10.1007/s12232-024-00449-8>
- [12] Galletta S, Mazzù S. ESG controversies and bank risk taking. *Business Strategy and the Environment*. 2023;32(1):274–288. <https://doi.org/10.1002/bse.3129>
- [13] Gangwani M, Kashiramka S. Does ESG performance impact value and risk-taking by commercial banks? Evidence from emerging market economies. *Business Strategy and the Environment*. 2024;33(7):7562–7589. <https://doi.org/10.1002/bse.3882>

-
- [14] Srairi S. The impact of risk and Fintech on ESG performance: evidence from Gulf Cooperation Council (GCC) banks. *Journal of Chinese Economic and Business Studies*. 2025;23(3):363–404. <https://doi.org/10.1080/14765284.2024.2428240>
- [15] Galeone G, Ranaldo S, Fusco A. ESG and FinTech: are they connected? *Research in International Business and Finance*. 2024;69:102225. <https://doi.org/10.1016/j.ribaf.2024.102225>
- [16] Fung DWH, Lee WY, Yeh JJH, Yuen FL. Friend or foe: the divergent effects of FinTech on financial stability. *Emerging Markets Review*. 2020;45:100727. <https://doi.org/10.1016/j.ememar.2020.100727>
- [17] Ringe WG, Ruof C. Regulating Fintech in the EU: the case for a guided sandbox. *European Journal of Risk Regulation*. 2020;11(3):604–629. <https://doi.org/10.1017/err.2020.8>
- [18] Johri A, Kumar S. Exploring customer awareness towards their cyber security in the Kingdom of Saudi Arabia: a study in the era of banking digital transformation. *Human Behavior and Emerging Technologies*. 2023;2023:2103442. <https://doi.org/10.1155/2023/2103442>
- [19] Berger AN, Curti F, Mihov A, Sedunov J. Operational risk is more systemic than you think: evidence from U.S. bank holding companies. *Journal of Banking & Finance*. 2022;143:106619. <https://doi.org/10.1016/j.jbankfin.2022.106619>
- [20] Eisenbach TM, Kovner A, Lee MJ. Cyber risk and the U.S. financial system: a pre-mortem analysis. *Journal of Financial Economics*. 2022;145(3):802–826. <https://doi.org/10.1016/j.jfineco.2021.10.007>
- [21] Pavlidis G. Deploying artificial intelligence for anti-money laundering and asset recovery: the dawn of a new era. *Journal of Money Laundering Control*. 2023;26(7):155–166. <https://doi.org/10.1108/JMLC-03-2023-0050>
- [22] Goo JJ, Heo JY. The impact of the regulatory sandbox on the Fintech industry, with a discussion on the relation between regulatory sandboxes and open innovation. *Journal of Open Innovation: Technology, Market, and Complexity*. 2020;6(2):43. <https://doi.org/10.3390/joitmc6020043>
- [23] International Monetary Fund. Saudi Arabia: Financial Sector Assessment Program – financial system stability assessment. *IMF Country Report No.* 2024/281. Washington, DC: IMF; 2024. <https://doi.org/10.5089/9798400288074.002.A001>
- [24] Khan A, Malaika M. Central bank risk management, fintech, and cybersecurity. *IMF Working Paper No.* 2021/105. Washington, DC: IMF; 2021. <https://doi.org/10.5089/9781513582344.001>
- [25] Zuhroh I. Mapping Islamic bank governance studies: a systematic literature review. *Cogent Business & Management*. 2022;9:2072566. <https://doi.org/10.1080/23311975.2022.2072566>
- [26] Nguyen QK. Audit committee structure, institutional quality, and bank stability: evidence from ASEAN countries. *Finance Research Letters*. 2022;46:102369. <https://doi.org/10.1016/j.frl.2021.102369>
- [27] Liu Z, Li X. The impact of bank fintech on ESG greenwashing. *Finance Research Letters*. 2024;62:105199. <https://doi.org/10.1016/j.frl.2024.105199>
- [28] Zaid MAK, Khan MF, Ahmed A, Gelaidan HM, Al Koliby IS. Does environmental finance matter for sustainability? The role of financial innovation and Fintech. *Discover Sustainability*. 2024;5:500. <https://doi.org/10.1007/s43621-024-00686-5>
- [29] Nocoñ A. ESG risk management in banks—towards its measurement. *Economics and Environment*. 2024;90(3):737. <https://doi.org/10.34659/eis.2024.90.3.737>
- [30] Jain R, Kumar S, Sood K, Grima S, Rupeika-Apoga R. A systematic literature review of the risk landscape in Fintech. *Risks*. 2023;11(2):36. <https://doi.org/10.3390/risks11020036>
-