



In this Edition

SAMA Rewrites Derivatives Rulebook and Opens Saudi Market to Foreign Investors

Qatar Becomes First GCC Country to Adopt ISSB Sustainability Standards

Kuwait's CBK Launches Cyber and Operational Resilience Framework (CORF)

RBI Rolls Out Risk-Based Deposit Insurance and Tightens NBFC Norms

FRM Regulatory Pulse

Decoding emerging regulatory signals and risk priorities across global banking markets and their implications for risk, capital and resilience.

OUR QUARTERLY NEWSLETTER

May 2026

EXECUTIVE SUMMARY

This first edition of the Uniquis 'Regulatory Pulse' bulletin is designed to provide a structured view of key regulatory developments and supervisory themes across India and the Middle East.

The introductory edition covers developments observed over the quarter ended March 2026 and focuses on selecting jurisdictions where regulatory change and supervisory signals are most relevant to banking institutions and financial market participants.

Given the breadth and evolving nature of financial sector regulations, this publication focuses on banking regulators and core lending institutions. It does not seek to provide an exhaustive account of all regulatory developments, cover quasi-regulatory bodies, fintech regulators, GIFT-city-specific regulations, or other sectoral authorities within each jurisdiction. Instead, it concentrates on high-impact regulatory signals and supervisory priorities from banking authorities that are likely to influence risk management, governance, and balance sheet strategy.

The quarter reflects a tightening yet adaptive supervisory environment across key banking markets. Regulators are refining prudential frameworks, including capital, buffers, and macroprudential tools, while sharpening expectations on AML/CFT, conduct, and operational resilience. The direction of travel is clear, targeted recalibration to close observed gaps and reinforce risk-sensitive, data-driven supervision.

For boards and senior management, the implication is clear: a transition toward integrated, outcome-focused risk management. Institutions will need to demonstrate end-to-end control effectiveness,

operational resilience, robust capital planning, and strong data governance to meet evolving supervisory expectations. This bulletin highlights these cross-market signals, enabling firms to anticipate change and prioritize their risk and regulatory agendas accordingly.

Supervisory Themes at a Glance

The regulatory environment is no longer about ticking boxes; it is about proving control effectiveness.

Across India and the Middle East, several defining supervisory themes are emerging. Regulators are collectively moving from framework compliance to demonstrable control effectiveness, and institutions are expected to evidence outcomes rather than merely maintain policies. Data governance and reporting standardization have become central priorities, spanning derivatives reporting, sustainability disclosures, and liquidity metrics.

Operational and cyber resilience have been elevated to board-level governance disciplines, with formal maturity-based frameworks now in place across Kuwait, Qatar, and India. Capital tightening is measured but deliberate, evident in macroprudential adjustments in the UAE and in the redefinition of concentration risk in India.

The rapid expansion of digital payments and fintech infrastructure across Bahrain, Qatar, and India is driving heightened AML/CFT and transaction monitoring expectations. Financial innovation, while encouraged, is increasingly expected to operate within clearly defined regulatory boundaries.



IN THE NEWS

SAUDI ARABIA

SAMA Rewrites the Derivatives Rulebook: UPI Mandate, T+1 Reporting, and 2026 Backloading Clock

The Saudi Central Bank (SAMA) has implemented Version 4.0 of its [Trade Repository Reporting and Risk Mitigation Requirements for OTC Derivatives Contracts](#)¹, effective 1 February 2026. The framework replaces the prior regime and mandates the adoption of the Unique Product Identifier (UPI) under ISO 4914, aligning Saudi Arabia with global derivatives data standards and strengthening supervisory expectations for reporting discipline.

All locally licensed banks, including foreign branches, must report new, modified, and terminated OTC derivatives directly to a SAMA-authorized trade repository on a T+1 basis. Third-party reporting agents are no longer permitted.

Key structural shifts include:

- Mandatory UPI (or ISIN) reporting for all relevant OTC products
- Prescribed UTI format ("E02" + 20-character LEI + unique code)
- Defined single-sided reporting logic for certain cross-border transactions
- Lifecycle event reporting across modifications, corrections, early terminations, compression events, and daily valuation updates
- Hard backloading deadline of 31 December 2026 for legacy trades



Key implications

- Banks without direct repository connectivity and UPI enrichment by December 2026 face regulatory non-compliance risk and supervisory scrutiny.
- Operational disruption from non-compliance creates data integrity gaps, reducing supervisory visibility into OTC exposures and increasing systemic risk blind spots.
- Banks will need to strengthen governance and controls for non-centrally cleared OTC derivatives, including documentation, valuation, reconciliation, compression, and dispute escalation procedures.



Event Sponsorship Now Within SAMA's Regulatory Perimeter

The Saudi Central Bank (SAMA) has issued [Circular 472033844²](#) establishing a formal framework governing how supervised institutions organize, co-organize, and sponsor conferences, forums, and similar events.

The circular introduces defined internal approval, permit, and documentation requirements and clarifies expectations for event participation and sponsorship activities. Event-related engagements are now explicitly within SAMA's supervisory scope.

Core elements of the framework include:

- Clear governance parameters for organizing or sponsoring events
- Defined supervisory expectations around financial and non-financial sponsorship
- Formal approval and notification processes, where applicable

Opening of Saudi Arabia's Capital Market to All Foreign Investors (Effective February 1, 2026)

Saudi Arabia's Capital Market Authority (CMA) has officially [opened the Kingdom's capital market to all foreign investors³](#), giving them direct access across every market segment from February 1, 2026. The change does away with the Qualified Foreign Investor (QFI) framework that previously governed foreign participation in the Main Market, and there are no more eligibility hoops to jump through. The reform also removes the swap agreement framework, shifting foreign investor access from indirect/synthetic exposure toward direct ownership.

This represents one of the most significant structural shifts in Saudi capital markets in recent years, forming a central pillar of the Kingdom's Vision 2030

agenda to deepen market integration and attract international capital.

The liberalization covers the full breadth of the market:

- Equities on the Main Market (Tadawul)
- Sukuk, bonds, and other fixed income instruments
- ETFs and other listed investment products



Key implications

- Banks that treat event sponsorships as routine commercial decisions without formal governance approval expose themselves to supervisory scrutiny and enforcement action.
- Undocumented sponsorship activity could be treated as a control deficiency, inviting broader examination of governance frameworks.
- Reputational exposure is real: association with events outside SAMA's defined parameters can quickly become a public supervisory matter.

The onboarding process has been streamlined, with international investors accessing markets through a standardized process via CMA-licensed brokers. ⁴



Key implications

- Greater foreign participation deepens market liquidity but also amplifies exposure to cross-border capital flows and associated volatility. As a result, liquidity management strategies need to be revisited.
- AML/CFT frameworks and transaction monitoring must be scaled to handle the higher volumes and greater diversity of foreign investor onboarding.
- Institutions slow to adapt their product and client servicing models will find themselves losing ground to better-positioned international competitors entering the market.
- For customers, wider access to markets improves investment choices but also brings pricing dynamics and volatility not previously seen in a more restricted environment.

UNITED ARAB EMIRATES

AML/CFT framework refreshed - stronger emphasis on control effectiveness

The UAE has updated its AML/CFT and proliferation financing framework through [Federal Decree Law No. \(10\) of 2025⁴](#) and [Cabinet Decision No. \(134\) of 2025⁵](#). The CBUAE has anchored its [AML/CFT supervision⁶](#) to this updated legislative package. Recent CBUAE enforcement actions, including within the remittance and exchange segment, reinforce that deficiencies in AML/CFT controls may result in financial and reputational consequences. The updated framework, combined with ongoing supervisory activity, underscores the importance of demonstrable compliance with statutory requirements.

The updated framework makes clear that supervisory focus extends beyond documented policies to the effective implementation of risk-based customer due diligence, transaction monitoring, and reporting controls. Institutions are expected to demonstrate calibration of monitoring scenarios, thresholds, and alert-handling processes, with governance structures clearly demonstrating escalation, oversight, and remediation.

New CBUAE “umbrella” law - regulatory perimeter consolidated

[Federal Decree Law No. \(6\) of 2025⁷](#) on the Central Bank and the regulation of financial institutions, financial activities, and insurance business now serves as the primary legislative reference across [CBUAE rulebook updates⁸](#). The law provides the statutory foundation for subsequent rulebook instruments and regulatory requirements applicable to licensed entities.

For banks, the principal execution consideration is structured change management: ensuring that licenses, internal policies, governance artefacts and control frameworks are aligned with the updated statutory architecture as legacy references are rationalized or replaced.

Institutions operating across onshore, free-zone, and cross-border structures should ensure that regulatory mappings remain accurate and consistent across entities.



Key implications

- Institutions with policy frameworks but weak operational controls face enforcement action, including fines, license restrictions, or reputational damage.
- Failure to evidence calibrated transaction monitoring exposes banks to liability for undetected financial crime flows passing through their systems.
- Customers of non-compliant institutions face potential account disruptions and reputational spillover from enforcement actions.



Key implications

- Banks that do not update internal policies and governance frameworks to reference the new legislative architecture risk operating under outdated control structures.
- Inconsistent regulatory mappings across onshore, free-zone, and cross-border entities create compliance gaps that may be flagged during supervisory review.
- Failure to manage this transition in a structured way increases legal and regulatory risk, particularly for institutions with complex multi-entity operating models.

Macroprudential update – CCyB at 0.50% activated, then temporarily released

The CBUAE Rulebook⁹ activated the countercyclical capital buffer (CCyB) on UAE private-sector credit exposures at 0.50%, effective 1 January 2026, following a 12-month phase-in period that began on 1 January 2025. The buffer must be met solely through Common Equity Tier 1 (CET1) capital and applied as a “positive cycle-neutral” buffer in a neutral risk environment.

On 17 March 2026, however, the CBUAE Board approved a **Financial Institution Resilience Package**¹⁰, backed by CBUAE assets of approximately AED 1 trillion, which temporarily released both the CCyB and the Capital Conservation Buffer (CCB) to support the UAE economy amid extraordinary global and regional circumstances. The release forms Pillar III of a five-pillar package that also covers monetary policy measures, liquidity and stable funding relief, loan classification flexibility, and continued lending support.

Digital Dirham and mBridge - CBDC framework progresses

CBUAE publications on the **Digital Dirham**¹¹ and its participation in the mBridge wholesale CBDC platform outline a two-tier ecosystem in which regulated intermediaries distribute and interface with clients, while the central bank retains control over issuance and settlement.

The development of CBDC infrastructure introduces operational and governance considerations for participating institutions. The Digital Dirham retail pilot went live in November 2025, with broader rollout across peer-to-peer, commercial, and cross-border use cases through 2026 and full LFI support expected by year-end.

Onboarding, identity verification, and transaction processing must align with CBDC-specific roles. Integration between digital currency rails and existing AML, compliance, and sanctions frameworks must be clearly defined. Governance responsibilities across issuance, distribution, and settlement functions must be unambiguous within the two-tier structure.



Key implications

- The temporary release frees up significant CET1 headroom across the system; institutions should treat the relief as time-bound and continue to plan capital reinstatement scenarios as part of ICAAP and stress testing.
- Loan classification flexibility under the package does not suspend underlying credit risk monitoring; institutions still need robust IFRS 9 staging governance and clear documentation of “affected borrower” criteria to defend regulatory treatment when buffers are restored.
- The release is explicitly conditional on the macroprudential environment; institutions that read this as a permanent loosening risk material capital shortfalls if the CCyB is reinstated rapidly in response to changing conditions.



Key implications

- Institutions that delay preparation for CBDC integration risk being operationally unready when the Digital Dirham is more broadly deployed, creating a competitive disadvantage.
- Inadequate alignment between CBDC rails and AML/sanctions frameworks exposes banks to financial crime risk within new payment channels.
- For customers, a fragmented CBDC rollout with poorly prepared intermediaries creates friction, erodes trust, and limits the utility of digital currency as a payment tool.

QATAR

Sustainability Reporting Framework (SRF) - structured disclosure expectations

The Qatar Central Bank (QCB) issued a [Sustainability Reporting Framework \(SRF\)](#)¹² in December 2025, aligned with IFRS S1 (General Requirements for Disclosure of Sustainability-related Financial Information) and IFRS S2 (Climate-related Disclosures) - the ISSB Standards. Implementation commenced on 1 January 2026 under a phased approach with transitional reliefs designed to support institutions' readiness. The SRF positions Qatar as the first GCC country to formally adopt ISSB Standards via its central bank's regulatory framework. Disclosures span four core areas: governance, strategy, risk management, and metrics & targets.

Institutions must ensure governance arrangements supporting sustainability disclosures are clearly defined, data collection methodologies for portfolio-level metrics are documented and controlled, and that internal reporting, public disclosures, and risk management views remain consistent and reconcilable.

Institutions that treat SRF as a compliance task will struggle; institutions that embed SRF into portfolio governance (limits, pricing, sector appetite, and client engagement) will be able to defend both performance and disclosures as scrutiny rises.



Key implications

- Treating the SRF as a compliance checkbox is the wrong approach. Institutions that embed sustainability into portfolio governance will be far better positioned as scrutiny rises.
- Greenwashing risk is real, and growing discrepancies between public ESG disclosures and internal risk positions are attracting regulatory and legal attention across markets.
- Sustainability-linked financing is increasingly contingent on disclosure quality. Investors and counterparties are making decisions based on what institutions can evidence, not just what they claim.

Payment systems expansion - scale and control alignment

QCB's published [Payment Systems Statistics \(Retail Payment Systems\)](#)¹³ reflect continued growth in transaction volumes and expansion of instant and mobile payment channels. QCB's Payment Systems Statistics show 70.9 million transactions in March 2026 (+23% YoY), values more than doubling to QAR 150.9 billion, and instant transfer values up 124% YoY, driven by the Fawran service (3.77 million registered accounts). QA-RTGS and the late-2025 UPI integration have widened the rails further.

As transaction volumes increase and real-time rails expand:

- Customer authentication and fraud monitoring controls must operate effectively within compressed processing timelines.
- AML and sanctions screening processes should remain aligned with real-time transaction flows.
- Incident response and operational continuity arrangements should reflect the scale and speed of digital channels.

The published statistics underscore the structural shift toward digital payments, requiring institutions to ensure operational resilience and control effectiveness keep pace with throughput growth.



Key implications

- Real-time payment volumes are growing faster than most institutions' monitoring capabilities. As a result, the gap between throughput and control effectiveness is where financial crime risk accumulates.
- Downtime or processing failures in high-volume instant payment infrastructure carry disproportionate consequences given how systemically embedded these channels have become.
- Customers transacting through digital payment platforms with inadequate fraud controls face heightened exposure, leading to eroding trust, which is difficult to rebuild.

Data Handling and Protection Regulation - strengthened data governance expectations

The **QCB Data Handling and Protection Regulation**¹⁴ establishes requirements governing how financial institutions handle, store and protect customer and sensitive data. The framework addresses data governance, protection standards, and institutional responsibilities in relation to information security.

Data classification and ownership must be clearly defined, with controls over storage, transmission, and access aligned with regulatory expectations. Outsourcing and third-party arrangements must comply with applicable data protection requirements, and the monitoring and auditability of access to sensitive information must be documented.

Given the increasing digitization of financial services, alignment between data governance frameworks and regulatory requirements remains central to operational and cyber resilience.



Key implications

- Data classification and access controls are foundational, and without them, regulatory compliance is unverifiable, and cyber exposure is structurally unmanaged.
- Third-party arrangements without embedded data protection requirements are a liability that extends beyond the vendor relationship; the institution remains accountable.
- A data breach at an institution with inadequate governance is not just an IT incident; it is a regulatory event, a reputational crisis, and a potential legal liability all at once.



BAHRAIN

Bahrain advances fintech ecosystem with launch of Digital Direct Debit via Fawateer on BenefitPay

On 25 February 2026, BENEFIT - Bahrain's national fintech and electronic financial transactions service operator - launched a **Digital Direct Debit service via "Fawateer" through its BenefitPay¹⁵** app. The service replaces traditional paper-based mandate processes with API-based, instant mandate activation using verified customer credentials, and is fully compliant with ISO 20022 standards. It also supports automated reconciliation and integration with Enterprise Resource Planning (ERP) systems.

The launch is positioned as a foundational enabler for Open Banking, Open Finance, embedded finance, and account-to-account (A2A) payments in Bahrain, in line with the Central Bank of Bahrain (CBB) directives to modernize the digital payments infrastructure. BENEFIT processed BD 37.5 billion in electronic financial transactions across all transfer services in 2025, underscoring the platform's systemic relevance to the new service. For banks

and financial institutions, the expansion of digital payment rails increases the need for robust fraud detection, real-time transaction monitoring, and authentication frameworks.



Key implications

- New digital payment capabilities without upgraded fraud detection and monitoring are an open invitation for financial crime. Controls must scale with the channel, not lag behind it.
- Recurring payment authorizations via mobile introduce specific authentication vulnerabilities; without robust frameworks in place, liability exposure for the institution grows.
- Customers benefit from the convenience of digital direct debit, but that convenience quickly turns to distrust if fraud vectors are left unaddressed.

Bahrain raises \$2.1 billion through sovereign bond and Sukuk issuance

Bahrain issued a US\$2.1 billion dual-tranche **sovereign bond and Sukuk¹⁶** offering in February 2026, continuing its use of international capital markets to support government financing and liquidity management. The issuance comprised \$800 million trust certificates due 2034 and \$1.3 billion conventional notes due 2038, structured under Bahrain's existing global medium-term note program and Islamic trust certificate framework.

The transaction closed on 3 February 2026 and was listed on the Main Market of the London Stock Exchange. The Sukuk tranche was structured in accordance with Sharia principles under Bahrain's existing Trust Certificate Issuance Program, while the conventional bond tranche was issued under Bahrain's Global Medium Term Note Program. Joint lead managers on the offering were BNP Paribas, Emirates NBD Bank PJSC, First Abu Dhabi Bank PJSC, HSBC Bank plc, J.P. Morgan Securities plc, Mashreqbank psc, and National Bank of Bahrain.



Key implications

- Sovereign issuances of this scale absorb market liquidity. As a result, banks must monitor the impact on their own funding costs and liquidity positions accordingly.
- For banks active in regional debt capital markets, this signal continued sovereign deal flow and institutions without established capabilities risk being locked out of a growing revenue stream.
- Banks with high sovereign exposure concentrations should assess whether the additional supply affects portfolio risk and capital adequacy
- Sustained sovereign borrowing can crowd out private sector credit over time, potentially affecting lending rates and credit availability for customers

KUWAIT

CBK Launches CORF: A Structural Shift to Resilience-First Supervision

The Central Bank of Kuwait (CBK) has issued Version 1.0 of its **Cyber and Operational Resilience Framework (CORF)**¹⁷, replacing the 2020 Cybersecurity Framework and significantly expanding supervisory expectations.

CORF moves beyond baseline cybersecurity controls toward a resilience-centric, maturity-based oversight model. The framework spans six core components and introduces 876 controls across the cyber, operational resilience, and third-party risk domains.

Assessment is dual-layered:

- Control-level compliance (Compliant / Non-Compliant / N/A with CBK approval)
- A five-level maturity scale (Initial to Innovative)

Entities must submit a Statement of Applicability (SoA) before assessment, formalizing scope

and accountability at the Board and senior management level.



Key implications

- 800+ controls are not a minor update. Institutions that have not started a gap assessment are already behind, and remediation backlogs will only grow.
- Not submitting a Statement of Applicability itself is a governance failure. CBK will read it as a lack of board-level ownership over the framework.
- Immature cyber postures across interconnected institutions are not isolated risks; they create systemic vulnerabilities that affect the entire financial infrastructure.

Risk-Based Tiering Introduced: Oversight Calibrated to Systemic Impact

CORF establishes a structured **three-tier supervisory model**¹⁸, aligning assessment frequency with systemic importance and risk profile:

- Tier 1: Annual assessments (systemically important institutions and FMIs)
- Tier 2: 18-month cycle
- Tier 3: Biennial cycle

Tier placement is determined through a structured, inherent risk profiling that covers asset size, operational complexity, outsourcing exposure, cyber risk posture, and supervisory history. Importantly, classification is dynamic and may change following incidents, rapid digital expansion, or material operational shifts.

The tiering model formalizes supervisory intensity as risk-sensitive rather than calendar-driven. Additionally, an annual independent third-party

audit by a CBK-approved firm is mandatory for all regulated entities, in addition to CBK's own supervisory tiering.



Key implications

- Tier classification is dynamic; a single significant cyber incident or a period of rapid digital expansion could move an institution into a higher scrutiny tier without warning.
- Outsourcing exposure and cyber risk posture are active inputs into tier profiling. Institutions that do not manage these proactively are effectively letting CBK decide their supervisory burden for them.
- The tiering model is a positive systemic development: supervisory intensity is now proportionate to where the risk actually sits, improving market-wide oversight quality.

Third-Party Risk Elevated to Strategic Governance Priority

CORF's **Third-Party Risk Management (TPRM) Baselines**¹⁹ significantly expand regulatory expectations, comprising 13 domains and over 200 individual controls.

Scope extends beyond traditional vendor management to include:

- Board and senior management oversight
- Contractual safeguards and exit strategies
- Sub-contracting and fourth-party disclosure
- Cross-border compliance considerations
- Dedicated cloud governance requirements

Third-party risk is positioned as a core resilience pillar, reflecting CBK's emphasis on supply chain and outsourcing vulnerabilities within the financial system.



Key implications

- Fourth party and cloud exposures are now explicitly in scope; institutions still manage third-party risk through traditional vendor frameworks operating with a material blind spot.
- No documented exit strategy for a critical third party is not just a compliance gap; it is an operational crisis waiting to happen with no recovery path in place.
- Vendor incidents do not stay vendor problems: customers bear the consequences of service disruption and data exposure when third-party governance is inadequate.

Cyber Resilience Workforce Framework Formalized

Embedded within the CORF Toolkit, CBK introduces a structured **Cyber Resilience Workforce Framework (CRWF)**²⁰ that defines sector-specific job categories, competency benchmarks, and qualification expectations.

The framework defines standardized job categories, required skill sets, and qualification benchmarks tailored to regulated financial institutions. It is supported by two structured programs:

- Senior Cybersecurity Leadership Program (SCLP): Designed to enhance board and executive-level cyber governance awareness.
- Cybersecurity Resilience Assessor Program (CRAP): Establishes trained assessors capable of evaluating compliance with CORF and related standards.

Cybersecurity headcount and capability now form part of supervisory tiering considerations, linking workforce depth directly to oversight intensity.



Key implications

- Cybersecurity headcount and capability are now formal tiering inputs where under-resourced functions will translate directly into higher supervisory intensity.
- Board and executive cyber awareness are no longer assumed; they are now assessed. Leaders without adequate governance literacy are a documented vulnerability under CORF.
- Technology investment without the workforce to govern and operate it is not resilient. The market's collective cyber posture depends on building genuine human capability, not just deploying tools.



Operational Resilience Baselines Expand BCM Expectations

The **Operational Resilience Baselines (ORB)**²¹ introduce structured requirements across eight domains, covering:

- Governance and impact tolerance setting
- Business continuity management (BCM)
- Technology resilience and recovery
- Incident and crisis management
- Testing, training, and continuous improvement

Boards are expected to define impact tolerances and ensure that critical services are mapped to underlying systems and third-party dependencies. Scenario testing maturity will be explicitly assessed under the framework.

CORF represents a step-change in Kuwait's supervisory architecture. Cyber, operational resilience, and third-party governance are now integrated into a single maturity-based model with explicit board accountability and measurable supervisory benchmarking.



Key implications

- No board-approved impact tolerance means no baseline for resilience, and no baseline means the maturity assessment starts from the bottom.
- Scenario testing is not optional under ORB; continuity arrangements that have never been stress-tested will not hold up under either a real disruption or a supervisory review.
- When an institution fails during a stressful event, customers do not distinguish between a cyber-attack and inadequate planning; the reputational damage is the same.



OMAN

Oman strengthens BNPL regulation framework

The Central Bank of Oman has issued a regulation governing **Buy Now, Pay Later (BNPL) services**²², introducing a formal supervisory framework for institutions offering the product. The regulation establishes licensing procedures, capital adequacy requirements, disclosure standards, and risk management expectations to ensure that BNPL services are delivered in a transparent and disciplined manner.

The framework also includes consumer protection obligations and applies to all institutions licensed by the central bank to provide BNPL services. The move reflects growing regulatory attention to fast-expanding digital credit products and aims to ensure that appropriate risk controls and oversight support innovation in retail financing.

Oman banking sector expands as outlook stabilizes

Moody's²³ has revised the outlook on Oman's banking sector (Baa3) **from positive to stable**, citing expectations that non-oil GDP growth will remain around 3.5% in 2026, thereby sustaining loan demand. The agency expects loan quality to continue improving as economic growth supports borrowers' repayment capacity, while Omani banks maintain strong profitability and solid capital buffers. Higher oil production is expected to lift Oman's overall real GDP growth to 3.7% in 2026 from an estimated 2.6% in 2025. Moody's flagged overreliance on government deposits as a continuing structural risk, partially offset by strong liquidity buffers (problem loan coverage of approximately 129%) and the government's capacity to support banks in a crisis.

Separately, Fitch²⁴ has estimated Omani Islamic banking assets at approximately USD 24 billion (around RO 9.3 billion) at the end of 2025, with total Islamic finance industry assets nearing USD 36 billion, reflecting the continued role of Sharia-compliant finance in the broader sector. Additionally, Fitch projects total Islamic finance



Key implications

- BNPL activity now falls within a formal licensing perimeter, reducing scope for unlicensed or loosely governed providers to operate outside supervisory expectations.
- Capital adequacy and disclosure requirements exist for a reason: BNPL-driven consumer credit exposure, if left unmanaged, can accumulate faster than institutions realize.
- The consumer protection dimension matters: customers gain meaningful safeguards under this framework, but tighter eligibility criteria may also narrow access for certain segments.
- Unregulated BNPL growth is a household debt risk at scale; the framework addresses a gap that, unchecked, could have had systemic implications for financial stability.

industry assets will approach USD 45 billion in 2026 (from approximately USD 36 billion at end-2025), reflecting double-digit growth supported by regulatory reform and continued sukuk issuance.



Key implications

- Moody's signal is one of **stabilization, not improvement** - the move from "positive" to "stable" trims the upside narrative and suggests the rating agency sees less near-term ratings momentum than it did previously. Banks should calibrate investor messaging accordingly.
- Funding concentration in government and public-sector deposits remains the rating-relevant structural risk; institutions with elevated reliance on this segment should anticipate continued supervisory and analyst focus on liquidity diversification.
- Strong provisioning coverage and government support capacity remain the primary anchors for the stable outlook; any erosion in either would put ratings momentum back on the table.

INDIA

RBI amends NBFC Credit Risk Management Directions (governance & related party lending)

The RBI issued **Amendment Directions to the NBFC Credit Risk Management framework²⁵**, strengthening governance over **related party lending**, Board level oversight, and credit decision independence. The amendment introduces formal definitions, clarifies approval structures, and tightens documentation expectations for credit exposures involving connected parties.

NBFCs are expected to reassess Board-approved credit policies, related-party exposure monitoring, and internal approval committees to ensure the independence, traceability, and regulatory defensibility of credit decisions.



Key implications

- Related-party lending without robust governance is no longer a risk that regulators will overlook. The amendment signals that connected-party credit will be examined closely.
- Credit losses involving connected counterparties, where governance was demonstrably weak, carry reputational and legal consequences well beyond the financial exposure itself.
- Groups that have relied on captive NBFCs as intra-group liquidity providers face the sharpest adjustment as tighter related-party norms will curtail such flows, requiring either structural reorganization or a shift to external funding.

RBI aligns the definition of capital for NBFCs

The RBI on 10 March 2026 issued the **Second Amendment to the NBFC Concentration Risk Management Directions²⁶**, amending the Master Direction issued on 28 November 2025. The amendment, which comes into force with immediate effect, is primarily aimed at reviewing the definition of Tier 1 capital used for compliance with credit and investment concentration norms. As a parallel change, the definition of “Owned Fund” has also been harmonized with the NBFC – Prudential Norms on Capital Adequacy Directions, 2025.

The revised Tier 1 capital definition incorporates a specific proviso of Base Layer NBFC, “where an NBFC has augmented its capital, it must obtain an external auditor’s certificate confirming completion of the augmentation and submit it to the RBI’s Department of Supervision before reckoning the additions to capital funds for concentration-norm compliance”, which was earlier applicable only for Upper Layer. Separately, the Tier 1 Capital for testing single-borrower and single-group concentration limits must be determined based on the NBFC’s latest available financial statements, whether audited or subject to limited review.



Key implications

- NBFCs with consistent earnings and clean quarterly close processes can now expand concentration headroom on a quarterly cycle, directly supporting portfolio growth.
- Smaller, unlisted NBFCs without an established quarterly review process will effectively remain on an annual cycle, widening the operational gap between larger and smaller players in managing concentration headroom dynamically.
- Definitional alignment with the Capital Adequacy Directions, 2025, removes interpretive divergence between the two regimes - concentration computations and capital adequacy computations must now draw on a single reconciled capital base, simplifying internal reporting but raising the cost of any inconsistency.

RBI revises liquidity risk assumptions under the Basel III framework

The RBI issued amendments to the [Liquidity Coverage Ratio \(LCR\) framework](#)²⁷ on April 21, 2025, effective April 01, 2026, by increasing run off rates on digitally enabled retail deposits and refining haircuts on High Quality Liquid Assets (HQLA). The changes reflect evolving depositor behavior in a highly digitized financial system and the higher stress sensitivity of mobile-enabled deposits.

Institutions must reassess liquidity stress scenarios, behavioral assumptions, contingency funding plans, and the interaction between digital channels and liquidity risk.

RBI proceeds with stricter lending norms for brokers and proprietary traders

The RBI has confirmed implementation of [revised rules restricting bank lending to stockbrokers and proprietary traders](#)²⁹ effective April 2026. The framework includes tighter collateral requirements and restrictions on lending for proprietary trading activities.

[Industry associations have expressed concerns regarding liquidity impacts](#)³⁰; however, the RBI has indicated that the framework will proceed as planned.

The changes reflect RBI's supervisory focus on leverage and interconnectedness between banks and capital market intermediaries. Tighter norms may reduce the transmission of risk from capital markets into the banking system.

Banks may need to reassess exposures to capital market entities, including collateral frameworks, counterparty limits, and stress scenarios linked to market volatility. Reduced credit availability could also shift financing demand toward NBFCs and offshore lenders.



Key implications

- Digital deposits behave differently under stress. A higher run-off rate (an additional 2.5%) on internet and mobile banking deposits means banks must hold more (low-interest-yielding) HQLA to cover the regulator-prescribed outflows.
- G-Sec haircuts of 0.5%–6% under LAF/MSF norms reduce the effective value of Level 1 HQLA, requiring larger G-Sec holdings for Banks to maintain LCR compliance.
- Run-off rate on non-financial entities (trusts, partnerships) reduced to 40% from 100%, which is a partial offset to the above tightening measures.



Key implications

- The April 2026 deadline is confirmed; non-compliant exposures to brokers and proprietary traders need to be restructured now, not when the review cycle arrives.
- Beyond compliance, this is a portfolio risk question: institutions with concentrated capital market exposures need to stress-test how reduced broker credit affects counterparty risk and collateral adequacy.
- Reduced bank credit to capital market intermediaries narrows market liquidity and trading activity. As a result, the downstream effect on price discovery and market stability is real, if gradual.

Risk-based deposit insurance premium framework effective April 2026

The RBI introduced a **risk-based premium framework for deposit insurance**³¹ on February 06, 2026, effective April 2026, replacing the flat-rate premium system. Discounts will be given to Scheduled Commercial Banks based on their Risk Ratings (A, B, C, and D, with Category A representing the lowest risk) and vintage (1% per stress-free year, capped at 25%). Under the framework, an “A”- rated bank with over 25 years of stress-free vintage will see its premium decrease by 50% (i.e., 6 paise per Rs.100 of assessable deposits, down from 12 paise per Rs.100 of assessable deposits).



Key implications

- With the introduction of Risk-Based Premiums, weaker institutions forfeit the cost dividend that accrues to stronger peers, widening the relative operating cost gap over time
- Capital, asset quality, and governance discipline now have a quantifiable operating cost linkage.
- The confidentiality requirement around risk categories does not eliminate market signaling counterparties, and analysts will infer category placement from supervisory ratings, financials, and DICGC payments over time.
- The vintage incentive design rewards long-run stability; institutions emerging from restructuring or recent distress events should expect their incentive clock to be reset, with funding cost implications.

RBI establishes high-security data hub to strengthen systemic resilience

The RBI has established a **high-security data hub**³³ intended to protect critical banking infrastructure and ensure continuity of core financial system operations. The facility has reportedly been located in a geographically secure region to mitigate environmental and geopolitical risks.

This initiative reflects the central bank's focus on strengthening systemic operational resilience as financial infrastructure becomes increasingly digitized.

For banks, the broader context highlights the importance of:

- Disaster recovery and business continuity capabilities
- Dependency mapping of critical infrastructure
- Cyber resilience and data protection governance



Key implications

- The RBI is investing in systemic resilience. The expectation is that supervised institutions do the same. Disaster recovery and infrastructure dependency mapping are now baseline supervisory expectations.
- Cyber resilience and data protection governance that has not kept pace with RBI's direction will be increasingly visible during the supervisory cycle.
- A secure central data hub reduces concentration risk at the system level, but its effectiveness depends on the resilience of the institutions it connects to, making bank-level preparedness equally critical.

DISCLAIMERS

This publication has been prepared by Uniquis for general informational purposes only and is intended to provide a high-level overview of selected regulatory developments and supervisory themes across jurisdictions. It is based on publicly available information, including regulations, circulars, consultation papers, supervisory statements, research publications, and reputable media reports current as of March 2026.

The content does not constitute and should not be construed as:

- Legal, regulatory, tax, accounting, or investment advice
- A formal interpretation of law or regulation
- A comprehensive or definitive statement of the positions of any regulator or public authority

Readers are encouraged to seek appropriate professional guidance before taking any action based on the information contained in this document.

While reasonable care has been taken in compiling the information, Uniquis does not make any representation or warranty, express or implied, as to the accuracy, completeness or timeliness of the content. Regulatory developments are subject to change, interpretation and jurisdiction-specific application, and the information presented may not reflect the most current position in all cases.

This publication does not seek to provide an exhaustive account of all regulatory updates, quasi-regulatory guidance, or supervisory communications within each jurisdiction. The selection of topics reflects areas considered to be of broader relevance and does not imply materiality or priority in all contexts.

The views expressed are based on publicly available information and represent a general interpretation of regulatory developments. They do not represent the views of any regulator or authority and should not be construed as definitive interpretations of applicable laws or regulations.



ABOUT THE REGULATORS

The following are the official websites of the banking regulators and supervisory authorities covered in this bulletin:

- **Saudi Arabia**
 - [Saudi Central Bank \(SAMA\)](#)
 - [Capital Market Authority \(CMA\)](#)
- **United Arab Emirates** → [Central Bank of the UAE \(CBUAE\)](#)
- **Qatar** → [Qatar Central Bank \(QCB\)](#)
- **Bahrain** → [Central Bank of Bahrain \(CBB\)](#)
- **Kuwait** → [Central Bank of Kuwait \(CBK\)](#)
- **Oman** → [Central Bank of Oman \(CBO\)](#)
- **India** → [Reserve Bank of India \(RBI\)](#)

REFERENCES

The regulatory circulars, official publications, and reports cited throughout this bulletin are listed below:

1. SAMA Circular 472021766 - Trade Repository Reporting and Risk Mitigation Requirements for OTC Derivatives Contracts, Version 4.0 (September 2025 / effective February 2026)
2. SAMA Circular 472033844 - General Rules for Organizing and Sponsoring Events (November 2025)
3. CMA - Announcement on opening of capital market to all categories of foreign investors (effective February 1, 2026)
4. CBUAE Rulebook – Federal Decree-Law No. (10) of 2025 (AML/CFT & Proliferation Financing)
5. UAE Legislation – Cabinet Resolution No. (134) of 2025 (Executive Regulations) [PDF]
6. CBUAE – AML/CFT Supervision Overview
7. CBUAE Rulebook - Federal Decree-Law No. (6) of 2025 (Central Bank & regulation of financial institutions)
8. CBUAE – Legislation Page
9. CBUAE Rulebook - Countercyclical Capital Buffer (CCyB) section (0.50% effective 1 Jan 2026)
10. CBUAE Financial Stability Report 2024 (published 2025) [PDF] - reference to CCyB 0.5% as of 2026
11. CBUAE – CBDC / Digital Dirham Short Report [PDF]
12. Qatar Central Bank – Sustainability Reporting Framework (SRF) [PDF]
13. QCB – Payment Systems Statistics Landing Page
14. Qatar Central Bank – Data Handling and Protection Regulation [PDF]
15. TechAfrica News – Benefit launches Digital Direct Debit via BenefitPay (February 2026)
16. Baker Botts – Bahrain Dual-Tranche Sovereign Bond and Sukuk Offering (February 2026)
17. Central Bank of Kuwait – Cyber and Operational Resilience Framework (CORF) Version 1.0 (December 2025)
18. CBK CORF – Chapter 1, Section 10: CBK Oversight and Risk-Based Tiering (December 2025)
19. CBK CORF – Chapter 6: Third-Party Risk Management Baselines, Domains 1–13 (December 2025)
20. CBK CORF – Chapter 3, Section 9.3.3: Cyber Resilience Workforce Management (December 2025)
21. CBK CORF – Chapter 5: Operational Resilience Baselines, Domains 1–8 (December 2025)
22. Central Bank of Oman – BNPL Regulation
23. Oman Observer – Moody’s revises Oman’s banking sector outlook to stable
24. Oman’s Islamic finance sector poised to top \$45 billion in 2026 - Oman Observer
25. RBI Circular – NBFC Credit Risk Management Amendment Directions, 2026 (5 January 2026)
26. RBI Circular – NBFC Concentration Risk Management Second Amendment Directions, 2026 (10 March 2026)
27. RBI Circular – Basel III LCR: Review of Haircuts and Run-off Rates (21 April 2025)
28. RBI Notification – Guidance Note on Operational Risk Management and Operational Resilience
29. Reuters – India central bank not looking to revisit lending rules for proprietary traders and brokers (February 2026)
30. Reuters – Indian brokers lobby seeks 6-month freeze on new RBI rules (February 2026)
31. Risk-based Premium Framework for Deposit Insurance in India
32. Economic Times – RBI unveils risk-based deposit insurance premium framework
33. Times of India – RBI sets up high-security data hub in Odisha to protect core operations

About Uniquis Consultech:

Uniquis Consultech is a global tech-enabled consulting company that specializes in Accounting & Reporting, Governance, Risk & Compliance, Sustainability & Climate, Tech Consulting, and Valuations. The Company is co-founded by consulting veterans Jamil Khatri and Sandip Khetan and backed by marquee investors such as Nexus Venture Partners, Sorin Investments, and UST.

Uniquis has a global team of 800+ professionals led by 100+ Partners & Directors across eleven offices in the USA, the Middle East, and India. The company serves more than 300 clients, including marquee names in each of the markets it operates in.

Uniquis is committed to leveraging technology and an integrated global delivery model to provide best-in-class consulting services to its clients.

In today's volatile macroeconomic and regulatory environment, financial institutions are expected to anticipate, measure, and manage risks in real time. Frequent regulatory updates (Basel/RBI guidelines), evolving market dynamics, and complex products such as structured credit and derivatives are reshaping risk profiles. Heightened expectations from Boards, investors, and regulators around stress testing, ICAAP/ILAAP, and forward looking risk assessments demand robust models, high quality data, and agile risk infrastructure.

Our Financial Risk Management (FRM) practice is designed to partner with your risk and finance functions through this complexity. We help institutions strengthen their frameworks across credit, market, liquidity, and balance sheet risk covering policies, governance, models, and reporting. Our teams work as an extension of your in house risk function to design, implement, and validate risk models and frameworks, embed them into day to day decision making, and align them with regulatory expectations and your risk appetite.

To learn more about our FRM practice please [download our FRM Brochure](#).

Contributing Authors



Sagar Lakhani
Partner, Accounting & Reporting Consulting



Suresh Wadhwani
Partner, Financial Risk Management



Shyam Gupta
Associate Partner, Financial Risk Management



Govind Agarwal
Associate Director, Financial Risk Management



Manjunath Kattimani
Associate Director, Financial Risk Management

Shabri Mayekar, Manager, Financial Risk Management
Sarraha Bahrainwala, Manager, Financial Risk Management
Megh Nanavati, Assistant Manager, Financial Risk Management
Devash Joshi, Assistant Manager, Financial Risk Management
Aniket Asthana, Consultant, Financial Risk Management

Feedback

We encourage you to share this newsletter with your colleagues and networks, and to provide us with feedback on topics that you would like to see covered in future issues. Uniquis is here to support you in navigating this evolving landscape. Contact us to learn more about how we can help you on your sustainability journey.



Visit us at www.uniquis.com

or follow us on

