CONFIDENTIAL INVESTOR FOLLOW-UP RESPONSE

Technology Stack Narrative Layer-by-Layer Explanation

Accompanying note to the Akkad Digital Islamic Bank technology-stack diagram prepared for SM Capital

Field	Description
Prepared for	SM Capital authorized investment-review team
Prepared by	Akkad Digital Islamic Bank
Date	19 July 2026
Purpose	To explain the technology-stack diagram in plain business and technical language, including the role of ICSFS, Codebase / CBT Digibanc under evaluation, APIs, integrations, cybersecurity, infrastructure and agency banking.

Executive summary

Akkad's technology architecture is designed for a no-branch digital Islamic bank. ICSFS / ICS BANKS is the selected core banking direction. Codebase Technologies / CBT Digibanc is under evaluation as a possible specialist digital-channel, wallet, merchant, agency-banking and integration layer. The architecture must remain CBI-compliant, Iraq data-resident, cyber-secure, auditable, scalable and capable of supporting digital channels plus controlled agency/cash-access operations.

1. How to Read the Technology Stack

The diagram should be read from the customer and channel layer down to the regulated banking, integration, security and infrastructure layers. Each layer has a distinct role, but the operating model depends on all layers working together through controlled APIs, audit trails, monitoring, reconciliation and governance.

- Customer-facing channels create the digital experience and transaction initiation layer.
- Core banking records the official customer, account, product, GL, posting and regulatory data.
- API and integration layers connect the core to channels, payments, cards, AML, KYC, credit bureau, agent systems and reporting tools.
- Cybersecurity, identity, access management and monitoring must sit across all layers.
- Infrastructure, data residency, business continuity and disaster recovery are foundational controls, not optional back-office components.

2. Layer-by-Layer Explanation

Layer	Role in Akkad model	Current vendor / status	Key controls and dependencies
Core banking layer	System of record for customers, accounts, deposits, Islamic products, postings, fees, limits, GL/COA, statements and regulatory reporting.	ICSFS / ICS BANKS Islamic selected as the core banking direction.	CBI reporting, Islamic product configuration, GL/COA mapping, audit logs, user access, product accounting, data residency and DR readiness.
Digital channels layer	Mobile/web journeys for retail, SME and corporate customers, including onboarding, dashboards, transfers, cards, statements, service requests and notifications.	ICS digital capabilities and/or Codebase / CBT Digibanc under evaluation for specialist digital interfaces. Final scope depends on module selection and commercial proposal.	Arabic/English UX, e-KYC workflow, role-based access, transaction receipts, customer consent, accessibility, uptime and integration with the core.
Wallet, merchant and agency layer	Supports wallet use cases, QR payments, merchant acceptance, agent cash-in/cash-out, agent float, commissions and settlement.	Codebase / CBT Digibanc is under evaluation for wallet, merchant and agency-banking capabilities; not yet awarded.	Agent due diligence, cash controls, transaction limits, AML monitoring, settlement, reconciliation, customer receipts and fraud controls.
API and integration layer	Connects core banking, digital channels, payment rails, card systems, AML/sanctions, KYC, credit bureau, notifications, reporting and third-party services.	To be finalized through target architecture; Codebase Fintegrator concept and ICS integration capabilities require validation.	API security, authentication, encryption, logging, throttling, error handling, retry logic, reconciliation, data mapping and integration ownership.
CBI and payment integrations	Connects Akkad to required Iraqi banking/payment ecosystem components such as RTGS, ACH, cheque/image clearing, retail payment infrastructure, cards/ATM/POS and regulatory reporting.	Specific connectors and providers to be confirmed during implementation planning.	CBI compliance, settlement controls, payment monitoring, operational procedures, business continuity, dispute handling and regulatory reporting cadence.
Cybersecurity and information security	Protects customer data, channels, internal users, infrastructure, APIs and third-party access.	Control framework to be embedded across all selected vendors and internal operations.	IAM, MFA, encryption, SIEM/SOC monitoring, vulnerability management, penetration testing, endpoint controls, incident response, vendor access management and annual assurance.
Infrastructure, data residency and DR	Hosts the core, channels, integration services, databases, backups, monitoring and disaster-recovery capabilities.	Target deployment must satisfy Iraq data-residency and high-availability requirements. Final architecture to be confirmed with vendors and CBI expectations.	Tiered data center design, local processing of critical data, backup, RPO/RTO, HA, network resilience, Oracle/database management, DR testing and change controls.
Governance and operating controls	Ensures technology delivery is controlled, auditable and aligned with CBI, board, risk, compliance and financial requirements.	Akkad governance, vendor governance and implementation PMO to own controls.	Policies, SLAs, vendor due diligence, outsourcing controls, maker/checker, audit trail, reporting, acceptance testing and CBI readiness tracking.

3. Codebase / CBT Digibanc Position

Codebase Technologies / CBT Digibanc should be presented to SM Capital as a technology-evaluation candidate for the customer-facing and ecosystem layers, not as a selected core banking vendor. Akkad should complete module selection, technical workshops, integration validation, cybersecurity/data-residency review, implementation planning and commercial negotiation before treating Codebase as a final awarded vendor.

Question	Current position
Why Codebase is being considered	The submitted Digibanc material maps to Akkad's no-branch model through digital onboarding, retail/SME/corporate journeys, wallet, merchant, agent banking and API-led integration concepts.
What is not yet finalized	Module scope, financial proposal, integration design with ICSFS / ICS BANKS, hosting/data-residency model, SLAs, implementation plan, cybersecurity evidence and contractual obligations.
Investor message	Codebase is a credible adjacent digital-channel candidate under evaluation. It should not be interpreted as a final vendor award or alternative core banking selection.

4. Implementation Implications

- The minimum launch architecture should prioritize core banking readiness, digital onboarding, account services, payments readiness, cards controls, audit trails and regulatory reporting.
- Agency banking and cash-access rollout should be phased after agent due diligence, liquidity, settlement, AML and reconciliation controls are tested.
- Codebase / CBT, if selected, should provide a module-by-module proposal with integration assumptions explicitly based on ICSFS / ICS BANKS.
- All vendors must be assessed against CBI requirements, Iraq data residency, cybersecurity, DR, SLA, audit, outsourcing, incident management and exit provisions.
- SM Capital should distinguish between selected/evidenced stack components and candidates still under technology evaluation.

5. Caveat

This narrative is prepared for investor-review discussion and should be read together with the technology stack diagram, the technology stack report, the ICSFS evidence pack, the Codebase / CBT evaluation materials, and Akkad's CBI licensing documentation. Final architecture, module selection, implementation scope, vendor responsibilities and cost remain subject to Akkad governance approvals, vendor statements of work, CBI requirements and executed commercial agreements.