

Akkad Digital Islamic Bank

Technology Stack Report for SM Capital

Prepared for investment review following the initial SM Capital discussion.

Field	Details
Audience	SM Capital authorized investment-review team
Scope	Core banking, digital channels, APIs/integrations, information security, cybersecurity, infrastructure, data governance, operational resilience, and investor technology-readiness view
Status	Investor-facing synthesis enhanced with ICS BANKS / ICSFS vendor evidence, signed-contract references, technical proposal, system summary, hardware architecture, certifications, and CBI readiness documentation
Date	12 July 2026
Confidentiality	Confidential and for authorized SM Capital / Akkad Digital Bank review only

1. Source Basis and Report Positioning

This report is a consolidated investor-readiness view extracted from the Akkad work already completed across licensing, CBI readiness, prototype design, business planning, and financial modeling. It is intended to help SM Capital understand the technology thesis, expected stack, operating dependencies, evidence status, and risks requiring diligence before investment or launch.

Source Area	How it was used in this report
SM Capital data room structure	Aligned the report to the investor-requested technology stack section and overall four-part investor review framework.
Akkad digital banking prototype	Mapped retail, SME, and corporate digital journeys, onboarding, e-KYC steps, and channel features into the digital-channel architecture.
CBI digital-bank gap analysis/readiness register	Used to identify regulatory technology expectations, evidence gaps, assurance requirements, and priority controls.
Data architecture response	Used for data governance, data policies, information-security policy coverage, access management, IT operations, and technology dependencies.
BCP and DRP documents	Used for operational resilience, business continuity, disaster recovery, RTO/RPO evidence expectations, and cyber-recovery planning.

External integration / API workstream	Used for integration architecture, API gateway logic, third-party controls, payments readiness, and vendor governance.
Financial and business model work	Used to align technology investment roadmap with the no-branch digital operating model, agency/cash-access model, and launch-phase cost discipline.
ICS BANKS / ICSFS evidence pack	Used to confirm the named core banking and digital banking platform, licensed modules, API/ESB architecture, Oracle technology stack, hardware/DR assumptions, ISO certifications, references, and contract/proposal evidence.
Codebase Technologies / CBT Digibanc proposal pack	Used to evaluate a specialist digital interface, wallet, agency banking, merchant services, digital onboarding, and API-integration option. The review is explicitly treated as technology evaluation only, not final vendor selection or commercial award.
Public Codebase Technologies information	Used to cross-check public positioning around digital banking software, digital strategy consulting, and regional digital-finance capabilities. Public sources were considered alongside the proposal, not as a substitute for formal due diligence.

2. Executive Technology View

Akkad is positioned as a no-branch digital Islamic bank. The technology model is therefore not a support function; it is the bank's operating backbone. The reviewed ICS BANKS / ICSFS evidence pack materially strengthens the core-banking position because it identifies the proposed core banking and digital platform, licensed functional scope, infrastructure assumptions, integration standards, and vendor assurance evidence. The reviewed Codebase Technologies / CBT material adds a credible digital-channel and wallet evaluation path, but it remains under evaluation and should not be treated as final selection until Akkad confirms modules, architecture fit, commercial proposal, implementation scope, and contractual terms.

- Core banking: the named target platform is ICS BANKS® ISLAMIC Core Banking System by ICS Financial Systems Ltd. (ICSFS), with documentation indicating a perpetual software license for Iraq, initial 25,000 customer capacity with scalability, contract date of 22 May 2025, and a source-code escrow reference.
- Digital channels: the named digital platform is ICS BANKS® Digital Banking Platform, covering mobile/tablet and internet banking, digital onboarding, P2P/local transfers, account statements, beneficiary management, standing instructions, QR code, and Android/iOS support.
- Digital interface option under evaluation: Codebase Technologies / CBT Digibanc is being assessed as a specialist front-end, onboarding, wallet, merchant, agent-banking, and integration layer candidate. No financial proposal has been finalized because Akkad must first select modules and confirm target architecture.

- Agency banking and cash access: CashBridge/agency banking is expected to provide cash-in/cash-out and customer-support access points under bank responsibility, reconciliation, limits, monitoring, and agent-risk controls.
- Integration layer: the proposal references an Enterprise Service Bus, Open Banking API capability, REST/SOAP Web Services, ISO 8583 for ATM/POS, SWIFT, ISO 20022 / RTGS / ACH, Reuters, image clearing, and third-party interfaces.
- Security and resilience: vendor/system materials reference RBAC, least privilege, HTTPS/TLS, AES-256 encryption at rest, Oracle RAC active/active availability, main/DR hardware architecture, and ISO 27001 evidence.

3. Vendor Evidence Reviewed and Impact on Technology Position

The newly attached documentation changes the report from a planning-level technology note to a materially evidence-backed technology stack report. The following evidence should be highlighted to SM Capital.

Evidence	Technology Impact
AKKAD-TECH-CBS-2026-003 System Technical Summary	Confirms ICS BANKS® ISLAMIC Core Banking System, ICS BANKS® Digital Banking Platform, licensed modules, Oracle technology base, integration standards, and Iraqi market/vendor reference evidence.
ICS BANKS Digital - Akkad Digital Bank Technical Proposal V1.0	Confirms project-specific digital banking proposal, modular platform logic, Open Banking/API approach, BPM/DMS, Oracle architecture, security/fraud section, implementation/testing framework, and recommended hardware section.
ICS BANKS ISLAMIC Main Features	Supports functional breadth of Islamic banking, customer/accounts, financing, treasury, deposits, GL/accounting, remittances, reporting, and operational modules.
ICSFS Digital Banking Brochure and Mobile Samples	Supports digital-channel capabilities, mobile/internet banking positioning, customer-facing digital services, and mobile user-experience examples.
Signed contract / former Akkad contract files	Support contractual maturity and should be reviewed by legal/technical due diligence for scope, license, support, maintenance, source-code escrow, and implementation obligations.
Hardware architecture document	Provides a concrete main-site, DR-site, utility/test architecture based on Oracle Linux, Oracle Database 19c Enterprise Edition, Oracle WebLogic 12c, Oracle RAC, Red Hat/JBoss BPM, SAN/shared storage, and DR replication options.
ICSFS ISO certifications	Provides vendor-side certification evidence, including ISO 27001 information security

	management and ISO 9001 quality-management references.
CBT - Akkad Digital Banking Proposal dated 15 June 2026	Provides a digital-channel evaluation proposal covering Digibanc, digital identity and onboarding, retail mobile/web banking, merchant QR services, agency banking, optional corporate banking, Fintegrator integration, and technology stack. It is not a final commercial proposal.
CBT - Digibanc Wallet Proposition 2027	Provides wallet-specific evaluation evidence covering customer wallets, agent wallets, merchant wallets, digital wallet core, QR payments, multi-currency wallets, local cash-in/cash-out, fraud monitoring, and API integration concepts.

4. Target Technology Architecture

The recommended architecture is a layered digital-bank platform. Each layer should be independently governed but integrated through controlled APIs, logs, audit trails, and service-level monitoring.

Layer	Target Role
Digital experience layer	Retail, SME, corporate, BOD/back-office review interfaces, onboarding workflows, servicing journeys, notifications, and customer support. This layer may be delivered through ICS digital channels, Codebase / CBT Digibanc modules, or a controlled hybrid approach after final architecture and commercial evaluation.
Identity and onboarding layer	Application capture, ID scan, MRZ/OCR, facial recognition, liveness, OTP, KYC profiling, AML screening, back-office review, and approval/rejection workflow.
API and integration layer	API gateway, service orchestration, authentication, rate limits, third-party integrations, payment rails, agency banking integrations, credit bureau, AML/sanctions, SMS/email, and reporting feeds.
Core banking layer	Customer master/CIF, account ledger, deposits, financing, cards/account controls, GL/COA, limits, fees, profit calculations, reconciliation, and regulatory reporting source records.
Data and analytics layer	Operational data store, reporting mart, data lineage, data quality, MIS, audit evidence, regulatory reporting, risk analytics, and future AI/fraud analytics capability.
Security and resilience layer	IAM, RBAC, MFA, encryption/key management, WAF, SIEM/SOC, endpoint protection, vulnerability scanning, backups, DR, BCP, incident response, and evidence logging.

5. Core Banking Platform

The core banking platform should be treated as the system of record for the digital bank. The evidence pack now names ICS BANKS® ISLAMIC Core Banking System as the proposed system, with ICS Financial Systems

Ltd. as vendor. This improves the report materially because the stack is no longer described generically; it can be diligenced against actual vendor documents, contracts, modules, integration standards, infrastructure needs, and implementation obligations.

- Documented licensed scope includes core application, extended core back-end, smart mobile banking, BPM back-end, document management, SMS/email notification banking, open banking and third-party integrations, e-statement, and Nostro reconciliation.
- Core module evidence includes customer master data, multi-currency accounts, GL, account/customer relationships, KYC, customer 360 view, monitoring/block lists, IBAN/BBAN, fees, transaction processing, standing instructions, foreign currency buy/sell, balance freezing, Islamic Murabaha financing, Islamic savings account, profit distribution, and CBI reporting.
- Extended back-end evidence includes credit/facilities management, risk groups, customer facilities, guarantees/guarantors, facility details, MIS reports, international and local transfers, and P2P transfer support.
- Investor due diligence should verify exact licensed user/customer limits, implementation scope, maintenance terms, source-code escrow, service levels, customization assumptions, support obligations, and CBI acceptance criteria.

6. Digital Channels and Customer Journeys

The Akkad frontend prototype demonstrates the intended channel segmentation: individual banking, SME banking, and corporate banking. For investor purposes, this shows the target operating logic before full production build and should now be converted into a production-grade roadmap with security, data, audit, and API integration requirements.

Journey	Technology Implications
Individual banking	Mobile/web login, digital account opening, e-KYC, payments/transfers, cards, statements, alerts, savings wallet/pockets, QR/P2P features, referrals, and service requests.
SME banking	Business onboarding, company profile, document capture, stakeholder verification, operating account, payroll, supplier payments, maker-checker approvals, corporate cards, and delegated administration.
Corporate banking	RM-assisted onboarding, legal document review, board resolutions/mandates, multi-approval workflows, payment limits, corporate cards, treasury/payment operations, payroll batches, and audit registers.
Back-office	Onboarding queue, approve/reject/request-more-information, exceptions, KYC review, audit trails, SLA tracking, and operational reporting.

The production version should enforce secure session controls, MFA/2FA, transaction signing or risk-based authentication, device binding where appropriate, audit logs, user-role segregation, complaint handling, and channel monitoring.

7. Codebase / CBT Digital Interface Evaluation

Codebase Technologies / CBT has been reviewed as a strategic digital-interface and wallet candidate for Akkad, not as a finalized awarded vendor. The reviewed CBT materials position Digibanc as a modular digital banking and wallet platform covering digital onboarding, retail mobile/web banking, merchant services, agency banking, optional corporate banking, and an API/integration layer called Fintegrator. This aligns well

with Akkad's no-branch model and agency-banking strategy, but final adoption must be conditional on module selection, commercial proposal, integration design with Akkad's selected core, CBI requirements, cybersecurity review, data residency, implementation capacity, and contractual protections.

Evaluation Point	Investor-Ready Position
Current status	Technology evaluation stage only. Codebase / CBT is not yet presented as a final selected vendor or final contracted platform for Akkad.
Financial proposal	No final financial proposal is available in the reviewed materials. Pricing should only be assessed after Akkad confirms selected modules, number of users/customers, environments, implementation scope, integrations, support model, and licensing structure.
Module-selection dependency	Akkad still needs to decide whether it requires retail mobile/web, SME/corporate channels, wallet, merchant QR/payments, agency banking, Fintegrator middleware, or only selected components.
Architecture fit	The CBT proposal references TCS BaNCS as core, while the latest evidenced Akkad core stack references ICS BANKS / ICSFS. Therefore, integration assumptions must be revalidated against the final selected core banking system and not copied directly from the proposal.
Why Codebase is a strong candidate	Codebase is a regional digital-banking specialist with public positioning around digital banking software and digital transformation, and proposal evidence showing Digibanc capabilities across onboarding, mobile/web channels, wallet, merchant, agent, and API layers. This makes it a strong candidate for Akkad's customer-facing digital interface, subject to due diligence.
Public / External Source	How it supports the evaluation
Codebase Technologies public website - https://www.codebtech.com/	Publicly positions Codebase as a digital banking and fintech solutions provider, with Digibanc, digital customer experience, open banking/APIs, digital core banking, RegTech, SaaS, and customer success stories.
Blink public website - https://www.theblink.com/en	Provides independent public context for a digital-only banking experience in Jordan, including app-based onboarding, digital account opening, cards, payments, ATM cash access, security, and customer support logic. This supports the type of

	digital-channel outcome Akkad is evaluating, without replacing formal vendor due diligence.
--	---

- Strategic fit: Codebase's Digibanc proposition maps closely to Akkad's target operating model: digital account opening, mobile-first servicing, wallet, merchant QR, agency/cash access, and API-led integration.
- Regional fit: the proposal references MENA/Iraq-relevant experience and Arabic/Kurdish/localization considerations, which are important for an Iraq-based digital bank.
- Product fit: the wallet proposition includes customer, merchant, and agent wallets, local cash-in/cash-out, QR payments, bill payments, multi-currency support, fraud monitoring, and out-of-the-box APIs.
- Execution caveat: Codebase should be evaluated through a formal RFP/commercial process before investor reliance, including demonstrations, reference calls, integration proof-of-concept, security documentation, implementation plan, and CBI compliance mapping.
- Investor caveat: Until a commercial proposal is issued and modules are selected, Codebase-related costs should be treated as placeholder or scenario-based in the financial model.

8. API, Integration, and Agency Banking Layer

The integration layer is central to Akkad's model because a digital bank must connect channels, core banking, identity providers, payment systems, agency/cash points, compliance tools, and reporting platforms. The API layer should be controlled through an API gateway rather than unmanaged point-to-point integrations. The ICSFS proposal specifically references ESB/middleware architecture, Open Banking API capability, Web Services / microservices catalogue, API Gateway / WAF / Authentication Gateway, OAuth Gateway, role-based service authorization, and a web-services catalogue layer.

- Documented integration standards include ISO 8583 for ATM/POS, SWIFT, RTGS/ACH, ISO 20022 references, Reuters, stock markets, third-party applications, image clearing, REST/SOAP Web Services, and middleware standard interfaces.
- The CBT Digibanc proposal references Fintegrator as an integration and orchestration layer with open-banking compliant APIs, core banking connectivity, payments integration, card-management integration, KYC/AML connectors, fraud/risk system integration, communications, analytics/data feeds, and ERP/third-party connectivity. These claims should be validated through technical workshops and proof-of-integration.
- Recommended controls remain essential: OAuth2/JWT or equivalent authentication, mutual TLS for sensitive integrations, API keys/secrets vaulting, rate limiting, IP allowlisting, payload validation, idempotency keys, transaction reference uniqueness, audit logging, and API monitoring.
- Agency banking scope: agent onboarding, cash-in/cash-out, transaction limits, liquidity monitoring, AML/KYC controls, agent reconciliation, exception management, location controls, and bank-responsibility oversight.
- External services: SMS/email/WhatsApp notifications, AML/sanctions, credit registry/bureau readiness, e-KYC/OCR/MRZ/liveness provider, cybersecurity monitoring, and reporting/data tools.

9. Information Security and Cybersecurity

The cybersecurity model must be designed as a regulator-facing control environment, not only as technical tooling. The CBI readiness work points to the need for stronger evidence around IAM, encryption, SOC/SIEM, vulnerability management, audit trails, cyber incident handling, and independent review.

Domain	Expected Control Position
Identity and access	RBAC, least privilege, MFA, privileged access management, joiner/mover/leaver controls, periodic access recertification, and admin activity logging.
Data protection	Encryption in transit and at rest, key management, data classification, retention/deletion logs, privacy controls, and masking of sensitive data in non-production environments.
Application security	Secure SDLC, code review, dependency scanning, penetration testing, vulnerability remediation SLAs, API security testing, and production change approval.
Monitoring and response	SIEM/SOC, EDR, anomaly detection, incident response playbooks, regulatory notification logic, forensic readiness, and cyber tabletop testing.
Third-party security	Vendor due diligence, DPAs, security attestations, right-to-audit, incident notification clauses, annual assurance review, and exit strategy.

10. Data Architecture, Residency, and Governance

The data architecture documentation records a strong policy base, including 31 completed policies/frameworks across data architecture, IT governance, data governance, information security, access management, IT operations, outsourcing, and technology portfolio management. The policy base exists, but formal board approval and operational evidence must follow licensing and board formation.

- Core data controls: data architecture framework, data governance policy, classification/retention policy, data quality, lifecycle, integrity, lineage/metadata, and privacy policy.
- Technology governance controls: IT governance manual, change management, SLA management, SDLC, systems integration policy, asset management, IT risk, compliance, acceptable use, outsourcing, and technology portfolio governance.
- Regulatory focus: Iraq data residency, local data center/server arrangements for critical data and processing where required, Tier 3/high availability design, retention and deletion logs, and cyber-risk assessments.
- Investor diligence: confirm data-center design, hosting model, backup locations, encryption ownership, data export rights, reporting lineage, and regulator-access evidence.

11. Infrastructure, BCP, DRP, and Operational Resilience

The BCP and DRP documentation provides the base for operational resilience. The newly reviewed hardware document adds a concrete infrastructure baseline for the ICS BANKS core and digital banking stack. For a digital bank, this evidence is important because service interruption directly affects the whole bank, not only a branch channel.

- Main-site hardware evidence includes two production core database servers using Oracle Linux 8, Oracle Database 19c Enterprise Edition, 128GB memory, mirrored usable database storage, and Oracle RAC / Oracle Clusterware active-active mode.

- Main-site application evidence includes two production core application servers using Oracle Linux 8 and Oracle WebLogic 12c, with active-active operation through a hardware load balancer.
- Digital banking evidence includes separate production digital database servers, mobile application servers, service-provider application servers, and BPM servers using Red Hat Linux / JBoss, with DMS attachment storage requirements.
- DR-site evidence includes core database/application servers, digital database/application servers, BPM DR servers, and replication options including SAN-to-SAN replication or Oracle Data Guard. Required evidence before final launch: DR test results, BCP simulation results, cyber tabletop report, third-party recovery SLAs, failover evidence, and board/committee review minutes.

12. Technology Roadmap for Investor Review

The roadmap should be phased to reduce execution risk and align capital use with licensing, build, testing, and launch readiness.

Phase	Technology Focus
Phase 1: Licensing and architecture closure	Finalize core banking and channel architecture, CBI evidence matrix, vendor due diligence, data residency design, cybersecurity baseline, and implementation governance.
Phase 2: MVP build and integration	Configure core banking, build digital onboarding and channel journeys, integrate e-KYC/AML/payments/notifications, implement API gateway, and prepare data/reporting foundations.
Phase 3: Security and operational readiness	Penetration testing, vulnerability closure, DR/BCP testing, SOC/SIEM activation, access recertification, operational runbooks, reconciliation testing, and incident playbooks.
Phase 4: Pilot and controlled launch	Staff training, limited user pilot, agent/cash-access testing, customer-support readiness, regulatory reporting dry runs, audit evidence pack, and launch-governance signoff.
Phase 5: Scale and optimization	Expand products, agency/cash coverage, analytics, fraud monitoring, automation, open APIs, AI-assisted operations, and portfolio risk analytics.