The Association of Governance Risk & Compliance

2026

Building Trust in Digital Finance:

A Practical Framework for Regulatory Harmonisation and Institutional Readiness

A White Paper by Elias M. Tayeh, Founder & CEO, Cedratech Consulting Services Ltd. and the Association of Governance, Risk and Compliance (AGRC)

Table of Contents

Executive Summary

Digital finance is expanding rapidly across borders, driven by open banking, instant payments, and fintech innovation. Yet this growth exposes deep fragmentation: inconsistent regulatory definitions, divergent consent models, weak identity infrastructure, and competing technical standards create barriers to cross-border harmonisation and inclusive access. RegTech and SupTech promise continuous, data-driven supervision, but scaling remains constrained by structural gaps in data quality, legacy systems, and institutional capacity.

This white paper argues that sustainable digital finance rests on four interdependent pillars:

- **harmonisation** of cross-border rules and technical standards,
- **capacity** encompassing both human talent and technical infrastructure,
- **trust** embedded through security and consumer protection by design, and
- **market readiness** across financial institutions, microfinance institutions, non-bank financial institutions, and ecosystem participants.

Drawing from direct experience implementing open-banking platforms in Nigeria, supporting financial inclusion programmes across MENA, and leading donor-funded technical assistance projects in Jordan, Iraq, and North Africa, this paper identifies what works in practice: outcome-based regulation with proportional compliance tiers, interoperability treated as policy infrastructure rather than competitive afterthought, trust-by-design controls embedding consent and portability into products, and capacity building that transforms compliance from procedural burden to informed governance.

Key recommendations:

- **Regulators** should establish minimum technical floors (FAPI, ISO 20022, LEI identifiers), publish explicit proportionality tiers for KYC and monitoring, and harmonise operational resilience standards.
- **Financial institutions** must design for portability with exportable transaction histories and interoperable identifiers, embed trust controls including explainable AI and consent audit trails, and build inclusion playbooks with offline features and multilingual support.
- **Donors and technical assistance programmes** should co-fund interoperability tooling and conformance testing, prioritise capacity building bridging compliance and technology, and support incremental pilots that prove value before scaling.

The most enduring infrastructure in digital finance is not the platform or the API – it is the ecosystem of trained professionals and collaborative institutions who build and sustain trust together.

Section 1

Introduction

Open banking, instant payments, and cross-border digital finance are reshaping financial services globally. APIs now enable third-party providers to initiate payments and access account data. Real-time payment rails connect consumers, merchants, and institutions instantly. Fintech platforms deliver credit, savings, and insurance to previously excluded populations. This expansion promises greater financial inclusion, lower transaction costs, and accelerated innovation.

Yet the regulatory landscape has not kept pace. Different jurisdictions classify third-party providers inconsistently, define payment accounts differently, and impose conflicting consent and data-residency requirements. Technical standards fragment across regions – PSD2 in Europe, Account Aggregator in India, Open Finance in Brazil, and emerging frameworks in Nigeria and across MENA. The result is a patchwork that raises compliance costs, blocks cross-border interoperability, and leaves consumers uncertain about protection and recourse.

The challenge is balancing innovation and interoperability with inclusion and trust. Regulators must enable experimentation without compromising consumer safety. Financial institutions must modernise operations without excluding underbanked populations. Technical assistance programmes must build capacity in markets where identity infrastructure, data governance, and supervisory tooling remain nascent.

This white paper synthesises practitioner insights from implementing digital payment systems in Nigeria as Managing Director of a licensed Payment Service Provider, supporting microfinance and SME finance programmes across Jordan under technical assistance funded by German development agency GIZ, training central bank officials and financial institution executives in digital finance strategy, and advising regulators on open banking, credit scoring, and operational resilience frameworks. The analysis identifies recurring patterns – what fails, what works, and what can be replicated globally to strengthen digital finance ecosystems.

Section 2

Harmonisation, RegTech, and the Framework for Trust-Anchored Innovation

The Seven Barriers to Regulatory Alignment

Cross-border digital finance faces seven core barriers to regulatory alignment.

1. **Fragmented rulebooks and definitions** create inconsistent classifications for third-party providers – AIS, PIS, TPP, fintech gateways, account-to-account initiators – and divergent scopes for "payment account" and "customer data", producing passporting gaps and unclear liability allocation. In Nigeria, the Central Bank had not yet defined a uniform compliance path for open-banking operators when we launched a licensed PSP, PTSP, and Super Agent platform. We proactively pursued ISO 27001, NDPR (Nigeria's GDPR equivalent), and PCI DSS 4.0 to anchor operations in international best practice. Later, a binding ISO 20022 circular forced ecosystem-wide workflow refactoring – an enormous, costly adjustment that could have been avoided with earlier standardisation and predictable supervisory roadmaps.

2. **Divergent consent models** – one-time versus ongoing, purpose-bound versus broad permissions, inconsistent revocation mechanics – undermine uniform customer experience and cross-border auditability. In the same Nigerian project, customers had to physically visit bank branches and pay ₦50 to authorise linking their accounts to our open-banking app – contradicting our positioning as an instant A2A payment provider. Several commercial banks delayed reporting consent updates to the national switch (NIBSS), effectively retaining control over authorisation data and blocking transparency.

3. **Weak identity infrastructure** compounds the problem. Supporting financial institutions across MENA, onboarding refugees, displaced persons, and the under-banked remains difficult because many lack formal identification. For corporate onboarding, the absence of API-enabled registry

infrastructure makes real-time verification impossible, slowing financial inclusion and raising compliance costs.

4. **Competing API and security standards** fragment ecosystems. PSD2/OBIE, India Account Aggregator, Brazil Open Finance, and Nigeria Open Banking differ on tokenisation, mutual TLS, and event-notification models, forcing multinational institutions to maintain multiple compliance stacks simultaneously.

5. **AML/CFT asymmetries** – threshold differences, divergent sanction lists, inconsistent VASP definitions–create uneven treatment of cross-border transfers, especially in remittance corridors between developing and developed markets.

6. **Operational resilience inconsistencies** leave regulators without visibility over cloud concentration risk and outsourcing dependencies that span borders and service layers.

7. **Consumer protection variance** – disclosure formats, complaint-handling timeframes, dispute-resolution channels – differs widely, reducing trust and complicating recourse for cross-border users.

RegTech and SupTech: From Periodic Review to Continuous Supervision

RegTech and SupTech transform supervision from periodic review to continuous monitoring. API-based regulatory reporting replaces quarterly PDFs with near-real-time event feeds, enabling supervisors to monitor risks as they emerge. Data standardisation through common schemas and identifiers reduces reconciliation noise and makes cross-institution analytics feasible – instant outlier detection on fees, latency, outages.

Model-aware supervision tools maintain inventories of AI and machine-learning models, track lineage, and detect drift, allowing regulators to examine credit-scoring or fraud-detection algorithms with evidence trails rather than policy attestations. Graph analytics and pattern-mining catch fraud networks, mule accounts, and market abuse patterns that rule-based systems miss.

Privacy-enhancing technologies, such as tokenisation, differential privacy, and secure enclaves, enable data-minimised cross-border analytics while respecting confidentiality constraints. Machine-readable regulation translates policy into executable validation checks, shrinking the gap between rule publication and implementation.

Why Scaling Consistently Fails: Structural Barriers to Adoption

Scaling consistently fails due to structural barriers. Data quality and taxonomy gaps defeat automation. In Nigeria, consent status for bank account linking was not consistently reflected at the national switch, creating latency that undermined SupTech relying on timely telemetry.

Weak digital identity foundations block API-driven onboarding – across MENA, onboarding refugees and displaced persons with limited IDs exposed the ceiling. Legacy cores cannot emit event streams or support schema evolution; interfaces remain batch-only. Sandbox-to-production migration hits a wall when adapters do not exist.

Interoperability fragmentation multiplies integration costs. Model risk governance remains underdeveloped and supervisors expect auditability for AI/ML, but tools often lack versioning, bias testing, or human-in-the-loop controls. Alternative-data credit scoring, valuable for thin-file customers, lacks regulatory recognition. Procurement cycles, talent scarcity, and unclear ROI stall adoption.

A Framework for Trust-Anchored Innovation

Frameworks for balancing innovation and trust begin with outcome-based regulation. Regulate for outcomes – security, transparency, redress, service continuity – rather than prescribing identical methods. Implement risk-tiered compliance with proportional KYC/AML, graduated requirements as transaction values rise, and simplified tiers for low-risk uses preserving inclusion.

Treat **interoperability as policy infrastructure** – mandate open, royalty-free interface standards for domestic instant payments, QR codes, and A2A transfers with published access terms and conformance testing. Embed **trust-by-design controls:** standardised disclosures, consent receipts with simple revocation, clear liability and chargeback rules, 24/7 incident notification with remediation SLAs.

Establish **data portability and purpose-bound**

consent with human-readable and machine-readable formats, unified consent logs, easy export of transaction history, strong audit trails. Mandate **inclusive design** – offline/low-bandwidth modes, vernacular languages, accessibility features, agent networks, fee caps for small values, user education, dispute assistance. Implement **model governance for AI/ML** – documented inventories, explainability artifacts, bias testing, challenger models, monitored drift, clear accountability.

Pathways Forward: Minimum Technical Floors and Shared Protocols

Pathways forward include minimum technical floors: agree on FAPI 1.0 Advanced + OIDC + JARM/ mTLS, ISO 20022, and LEI identifiers as shared protocols. Introduce **unified consent artifacts**: portable, machine-readable consent receipts with standard revocation webhooks and audit trails.

Harmonise **incident schemas** with shared severity tiers and reporting templates. Create **risk-based AML/CFT bridges** through coordinated typology-sharing and analytics. Encourage **joint supervisory codebases** – cross-jurisdiction test suites and certification pipelines. Retain **proportional inclusion safeguards** with simplified KYC and low-value tiers ensuring inclusion is not sacrificed for compliance.

Start narrow with high-value “report once, use many” pipelines, such as incident reporting, outage SLOs, fee transparency, then expand to richer datasets. Co-develop machine-readable rules and test suites so firms self-validate before submission. Adopt vendor-neutral reference architectures with adapters, schemas, conformance tests to reduce lock-in and shorten timelines.

CTOs and decision-makers must remain cost-conscious and strategically pragmatic. RegTech and SupTech implementations should be architected for incremental scalability, avoiding monolithic, vendor-dependent solutions that become expensive bottlenecks as transaction volumes or regulatory requirements evolve.

The goal is not perfection at launch, but adaptable infrastructure that can absorb future complexity without requiring costly overhauls. Every technical choice, such as API design, data architecture, and integration patterns, should be evaluated not only for compliance efficacy but for total cost of ownership and operational flexibility over time.

Section 3

Digital Transformation, Human Capital, and Lessons from Technical Assistance

How Digital Transformation Rewrites Institutional Operations

Digital transformation rewrites the entire operational DNA of financial institutions. Data governance shifts from siloed, department-specific databases to integrated data lakes or hybrid clouds, requiring new governance routines for data lineage, retention, quality assurance, and regulatory access. Compliance teams must move from periodic sampling to continuous data validation and automated reporting.

Customer onboarding and KYC/AML replace manual verification and paper trails with eKYC, biometric authentication, and digital platforms. Compliance now depends on real-time screening – PEP, sanctions, adverse media – and algorithmic decisioning that must be explainable, logged, and auditable. **Operational risk perimeters** expand to include APIs, cloud vendors, fintech partners, and data processors, demanding dynamic risk mapping that integrates cyber, vendor, and operational risk metrics into unified dashboards.

Product delivery moves from annual release cycles to continuous integration and deployment, requiring new compliance routines for model validation, version control, testing, and release approvals, including risk-based fast lanes for low-impact updates. **Regulatory reporting** increasingly expects machine-readable reports and live dashboards, calling for RegTech integration – automated data extraction, tagging, and reporting workflows coordinating compliance, IT, and operations.

The Legacy Core Problem: Why 94% of Transformations Miss Their Timelines

Roughly 94% of financial institutions fail to meet digital transformation timelines, and data migration is often the main culprit. Legacy systems, while functionally robust, are architecturally rigid. Many

are built on monolithic codebases with hard-coded logic and decades of patchwork updates. Extracting, cleaning, and mapping data to modern environments is slow, expensive, and risky. Data models are inconsistent, leading to broken referential integrity.

Migration testing must be repeated multiple times under live conditions. Downtime windows are limited, forcing incremental cutovers that multiply cost and risk. Budget overruns and timeline slippage are almost inevitable because legacy cores were never designed for modular upgrades or external connectivity.

Generation 4 Core Banking: Architect for Change

Generation 4 core banking platforms built on microservices, containerisation, and open APIs, are architected for change. They plug into fintech ecosystems seamlessly via RESTful APIs or ISO 20022 interfaces. They allow component-level updates instead of full-system overhauls. Data models are standardised and extensible, easing migration and reporting.

Most importantly, they support upgrade-without-downtime cycles, enabling real transformation without paralysing daily operations. Institutions adopting Gen 4 cores experience significantly higher transformation success rates precisely because these systems were built to be updated, connected, and compliant by design, not bolted on after the fact.

Recalibrating risk management frameworks means moving from procedural to predictive risk management. Replace siloed risk units – credit, ops, cyber, market – with cross-functional platforms using unified risk taxonomies and shared controls. Adopt continuous control testing and live key risk indicators linked to core and cloud systems. Implement onboarding, certification, and monitoring regimes for third parties and API providers. Maintain model inventories with version histories, bias and drift testing, and formal explainability reviews. Treat cybersecurity and operational resilience as core components of prudential risk with clear RTO/RPO metrics and incident escalation rules.

The Human Dimension: Talent, Culture, and Organisational Readiness

Most digital transformations fail not only due to technical bottlenecks but because the people dimension is under-addressed. The human dimension is the real foundation. Transformation requires cross-disciplinary talent – data engineers who understand compliance, compliance officers who interpret analytics, risk managers who read API logs. Legacy teams often lack exposure to agile development, CI/CD cycles, or cloud-based supervision tools.

Moving from manual, control-heavy processes to data-driven, automated workflows challenges entrenched mindsets. Teams used to retrospective reviews must adapt to continuous monitoring and predictive risk alerts – a cultural shift requiring targeted training and sustained leadership engagement. Institutions must embed structured learning pathways covering RegTech, SupTech, digital risk governance, model validation, cybersecurity, and operational resilience.

Digital transformation redefines traditional roles: compliance becomes tech-enabled, operations become data-led, audit becomes real-time. Updating job descriptions, KPIs, and internal reporting structures ensures staff understand their new accountability. **Executive leadership must treat training not as cost but as risk mitigation investment.** Establishing a digital transformation office or centre of excellence coordinates technical migration with human-capital alignment, ensuring people evolve with systems – not after them.

Capacity Building in Practice: Training Central Bankers and Market Players

Capacity building transforms compliance culture and regulatory readiness. Professional training and structured knowledge-sharing shift mindset from passive compliance to proactive digital governance. When I delivered a course on “Legal, Economic, and Business Aspects of Payments Digitalisation” to senior central bank directors, these officials were genuinely surprised by dashboards and data interpretations drawn from their own country’s payments ecosystem.

The visualisation helped them see interconnections between policy decisions, market behaviours, and emerging technologies they had not recognised before. When we addressed complex subjects like CBDCs, cryptocurrencies, and open banking indirectly and constructively – without challenging institutional positions – we created a safe intellectual space for critical thinking.

By the end, several participants acknowledged they lacked specialised human capital to design frameworks for digital assets and crypto regulation, but the session reshaped their internal dialogue. They began viewing these areas not as threats but as policy challenges requiring systematic study. This shift, from avoidance to strategic curiosity, is one of the clearest indicators that professional training enhances regulatory readiness.

In another engagement, I delivered Digital Finance Strategy training for senior executives of financial institutions from a North African country. Initially, participants were competitors, banks and microfinance providers accustomed to guarding their data. As training progressed, content around

data sharing, interoperability, and ecosystem collaboration sparked a breakthrough. When they realised the lack of a common digital finance framework was collectively stalling their market's evolution, they began cooperating.

During the final group exercise, these institutions jointly drafted an advisory note proposing a national open-banking framework for their regulator – a symbolic yet powerful outcome. Training catalysed a shared compliance culture, turning competition into coordinated progress.

Learning environments build trust in ways formal meetings cannot. Well-facilitated professional training creates safe spaces where regulators and market players exchange views candidly, building mutual trust that becomes the foundation of regulatory coherence. Visualisation and contextualisation make regulatory discussions tangible – using country-specific data dashboards and real market examples lets participants see themselves in the data, making learning relevant, localised, and actionable.

Indirect engagement on sensitive topics works because approaching areas like crypto, CBDCs, or data governance through discussion rather than advocacy reduces defensiveness and encourages reflection, transforming resistance into strategic foresight. Training catalyses policy collaboration – collective exercises like simulating open-banking frameworks help participants practice consensus-building, the same skill needed for cross-sector policymaking.

Professional learning closes the human-capital gap faster than traditional recruitment or academic study, providing both knowledge and confidence to act. Most importantly, training builds compliance culture through empowerment, not enforcement. When

professionals understand why regulations exist and how digital transformation interacts with them, compliance becomes an informed choice, not a procedural burden.

Lessons from the Field: Technical Assistance in Jordan

- **Donor-funded technical assistance provides the laboratory where innovation meets regulation.** Working for three years with financial institutions, microfinance institutions, and non-bank financial institutions in Jordan under a Technical Assistance (TA) project supporting MSME and women-led business access to finance revealed clear patterns with global applicability.

- **Co-design with the whole ecosystem works.** We worked hand-in-hand with Financial Institutions (FIs), Microfinance Institutions (MFIs), leasing companies, and other market actors to co-create solutions instead of imposing templates. The collaborative structure of workshops, focus groups, and joint market research allowed each participant to see the bigger picture and align on shared objectives. Institutions began introducing new financial and digital finance products aligned with MSME and women-led business segments. Others launched agri-lease products and bundled services because they had access to market data and customer insights generated through joint TA exercises. By contrast, insurance companies, which insisted on operating in a "one-man-show" style, fell short and eventually withdrew. Their isolation highlighted a simple truth: coordination multiplies impact, while isolation limits it.

- **Standards and frameworks should be set early, not after the fact.** Common definitions and risk assessment standards must be agreed at the beginning, not after pilot results appear. Early standardisation across credit scoring, product design, and consumer protection saved time and created comparability between partners. When institutions later explored digital lending or mobile-based onboarding, this early alignment allowed seamless transition into standardised risk reporting and data aggregation – something many TA projects globally struggle to achieve when frameworks come too late.

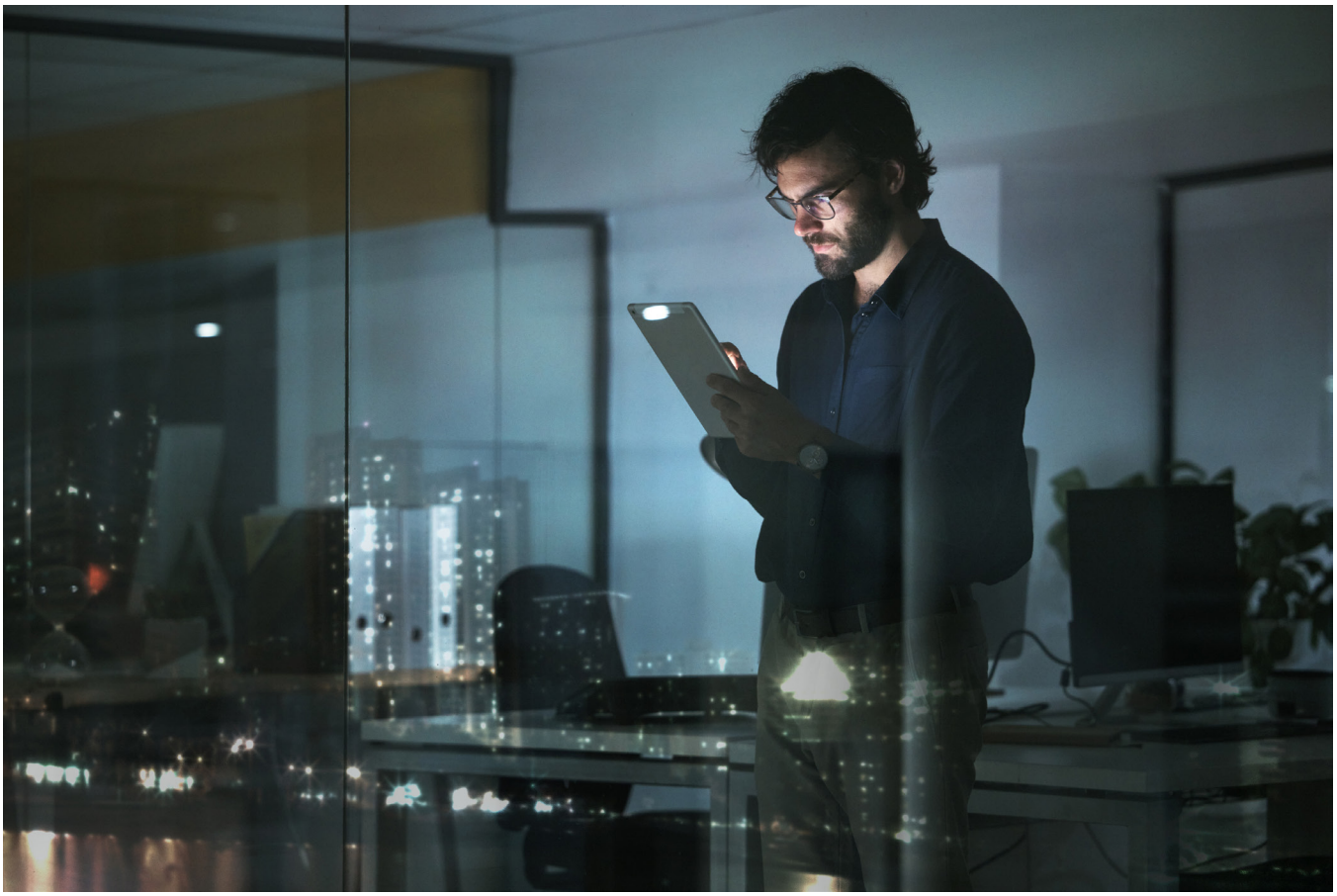
- **Identity, data, and human capital foundations are everything.** Even advanced digital tools mean little without verified identity systems, reliable data, and trained staff. In Jordan, onboarding small enterprises – especially informal or women-led ones – was challenging because of fragmented registries and non-digitised records. We coupled technical interventions with capacity building: training FI teams on assessing informal business profiles using proxy indicators, coaching them to combine market insight with compliance logic rather than relying purely on traditional collateral. This adaptive approach created a more inclusive credit culture.

- **Build consent and data governance from the start.** Even without formal open-banking rules, establishing transparent consent protocols and data-use disclosures was essential. Customers, especially women entrepreneurs, showed higher trust in institutions that could clearly explain how their information would be used. Data governance is not just a compliance checkbox; it's a business enabler that builds customer confidence and unlocks uptake.

- **Start narrow, ship value, then scale.** The Jordan project began with focused pilots, supporting one MFI in digital lending process re-engineering before scaling to others. This "start small, prove value" approach ensured lessons were internalised before wider rollout, allowing regulators and donors to demonstrate early wins, de-risk investment, and build stakeholder confidence.

- **Capacity first, capacity last.** No amount of technology can substitute for human readiness. Every successful deliverable – from new product launches to credit-scoring prototypes – was accompanied by training, coaching, and peer exchange. The difference between FIs that progressed and those that stagnated lay in how seriously they invested in their teams' understanding of digital finance and risk management.

The Jordan TA project's success was not about technology alone, it was about shared learning, coordinated execution, and human development. While insurers withdrew due to isolation, those who collaborated produced measurable outcomes: new MSME products, agri-leasing models, and digital finance offerings. This experience proves that sustainable digital transformation happens where collaboration, standardisation, and capacity intersect.



Section 4

Recommendations and Conclusion

For Regulators

Establish interoperability baselines requiring domestic schemes to support open APIs, standard QR codes, and account-to-account transfers with public conformance suites. This treats interoperability as critical infrastructure – like roads – lowering switching costs, preventing lock-in, and ensuring innovation competes on service quality rather than walled gardens.

Codify user protections through standardised disclosure templates, consent receipts with simple revocation mechanisms, and harmonised redress timelines across providers. Clear liability and chargeback rules, combined with 24/7 incident notification and remediation SLAs, build structural trust into products rather than relying on post-incident enforcement.

Publish explicit proportionality tiers for KYC, monitoring, and reporting to reduce ambiguity and speed approvals. Tiered regimes accommodate low-risk customers – offline/low-bandwidth modes, simplified verification, fee caps for small values – while foundational infrastructure like national eID and corporate registries matures. This ensures inclusion is not sacrificed for compliance.

Establish an operational resilience rulebook harmonising incident reporting, minimum SLOs covering RTO and RPO, standard incident tiers, and third-party risk expectations. Cloud and outsourcing transparency requirements, combined with periodic failover drills, ensure reliability becomes part of consumer protection. Innovation scales only when uptime, recovery, and vendor risk are governed.

Agree on minimum technical floors as shared protocols: FAPI 1.0 Advanced + OIDC + JARM/mTLS for API security, ISO 20022 for messaging, LEI identifiers for entity resolution. Introduce unified consent artifacts – portable, machine-readable consent receipts with standard revocation webhooks and audit trails. Harmonise incident schemas with shared severity tiers and reporting templates.

Create risk-based AML/CFT bridges through coordinated typology-sharing and analytics. Encourage joint supervisory codebases – cross-jurisdiction test suites and certification pipelines – to reduce duplicated certification and wasted resources.

For Financial Institutions

Design for portability from the outset. Implement exportable transaction histories, interoperable identifiers (LEI, standardised account references), and clear off-ramps to bank accounts or other wallets. This prevents lock-in, enables competition, and meets emerging regulatory expectations for data portability and purpose-bound consent.

Embed trust controls structurally. Bake in explainable decisions, model logs, and consent audit trails. Publish uptime and dispute KPIs transparently. Implement real-time monitoring dashboards integrating cyber, vendor, and operational risk metrics. Maintain model inventories with version histories, bias and drift testing, and formal explainability reviews. Treat cybersecurity and operational resilience as core components of prudential risk with clear RTO/RPO metrics and incident escalation rules.

Build inclusion playbooks addressing the hardest-to-reach first. Offer offline features, agent-assisted flows, and low-value fee relief. Provide multilingual support, vernacular interfaces, and accessibility features. Embed financial education content and dispute assistance. Design tiered onboarding accommodating customers with limited or non-traditional identification, using proxy indicators and market insight rather than relying purely on traditional collateral.

Invest in human capital and organisational culture. Embed structured learning pathways covering RegTech, SupTech, digital risk governance, model validation, cybersecurity, and operational resilience. Train cross-disciplinary talent – data engineers who understand compliance, compliance officers who interpret analytics, risk managers who read API logs. Update job descriptions, KPIs, and internal reporting structures so staff understand their new accountability in the digital ecosystem. Treat training not as cost but as risk mitigation investment. Establish a digital transformation office or centre of excellence coordinating technical migration with human-capital alignment.

Architect for incremental scalability. Avoid monolithic, vendor-dependent solutions that become expensive bottlenecks as transaction volumes or regulatory requirements evolve. Every technical choice from API design and data architecture to integration patterns should be evaluated not only for compliance efficacy, but for total cost of ownership and operational flexibility over time. The goal is adaptable infrastructure that can absorb future complexity without requiring costly overhauls.

For Donors and Technical Assistance (TA) Programmes

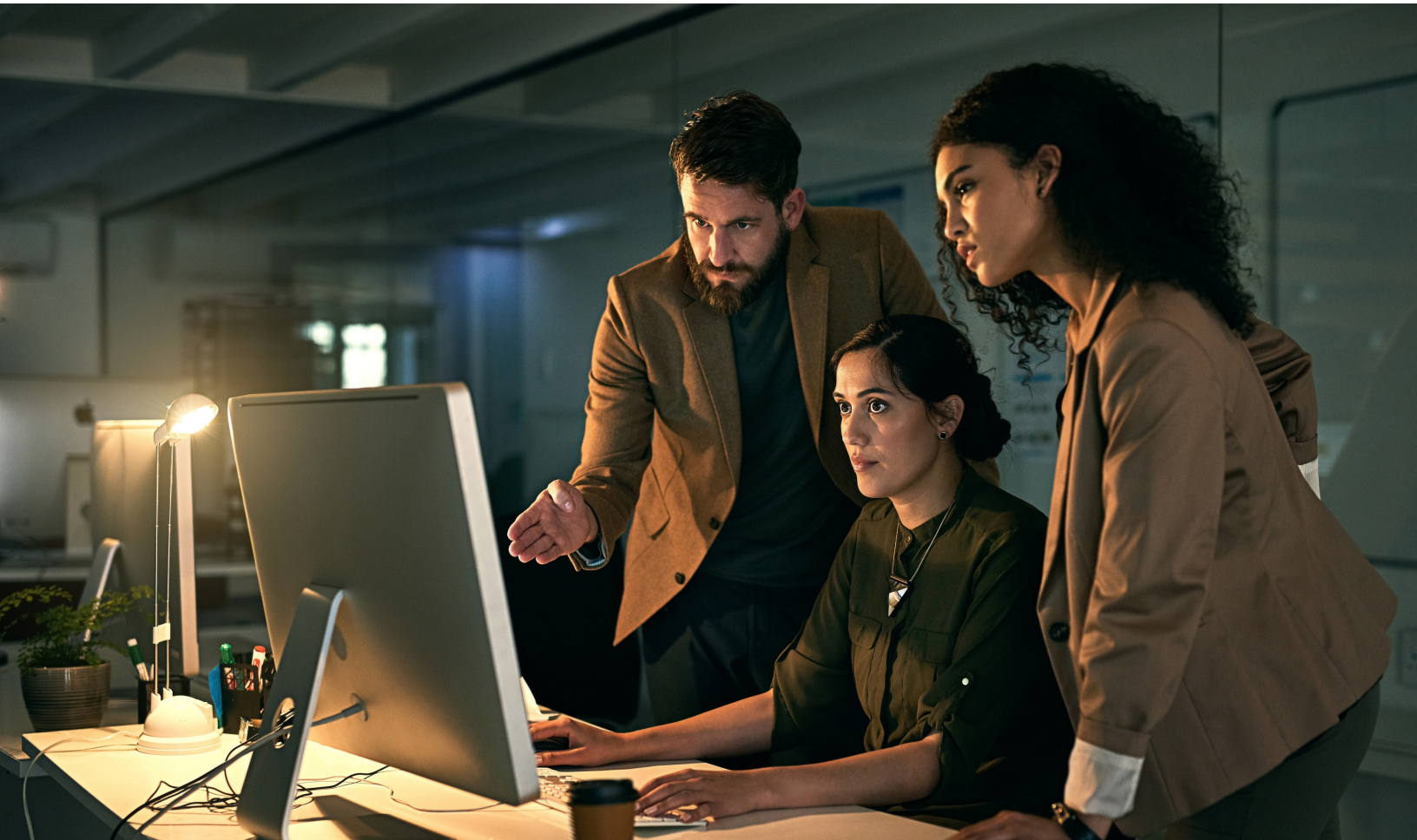
Co-fund interoperability tooling and conformance testing. Prioritise grants and TA for reference implementations, shared utilities – KYC/KYB rails, dispute resolution hubs, fraud and mule data-sharing, scheme-wide risk analytics – and privacy-enhancing technologies (tokenisation, differential

privacy, secure enclaves) that level the field for smaller providers and enable data-minimised cross-border analytics.

Prioritise capacity building bridging compliance, technology, and business lines. Train supervisors and providers on machine-readable rules, model risk management, and inclusive product design. Facilitate learning environments where regulators and market players exchange views candidly, building mutual trust that becomes the foundation of regulatory coherence. Use country-specific data dashboards and real market examples to make regulatory discussions tangible, relevant, localised, and actionable.

Support incremental pilots that prove value before scaling. Start narrow with focused interventions – supporting one MFI in digital lending process re-engineering, one leasing company in agri-lease product launch – ensuring lessons are internalised before wider rollout. This "start small, ship value, then scale" approach allows regulators and donors to demonstrate early wins, de-risk investment, and build stakeholder confidence.

Facilitate co-design with the whole ecosystem, including regulators, FIs, MFIs, NBFIs, leasing companies, fintech providers, and market infrastructures. Collaborative structures like workshops, focus groups, and joint market research allow participants to see the bigger picture and align on shared objectives. Coordination multiplies impact, while isolation limits it. Establish common definitions and risk assessment standards early – not after pilot results appear – to save time and create comparability between partners.



Closing Argument

Sustainable digital transformation happens where collaboration, standardisation, and capacity intersect. Technology may drive change, but trained, adaptive professionals sustain it. Gen 4 core banking platforms make digital transformation structurally easier; human capability development makes it operationally possible. Both must evolve together, because transformation that outpaces people inevitably fails to deliver its promise.

The most enduring infrastructure in digital finance is not the platform or the API. It is the ecosystem of people and institutions who build and trust it together. Interoperability treated as policy infrastructure, trust embedded by design, and capacity building prioritised as the foundation of regulatory readiness – these are the mechanisms through which innovation, inclusion, and governance advance in tandem.

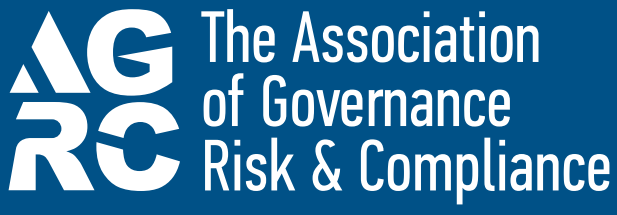
Early in my career, I helped build a route-management and collections digital tools in the UAE that worked well but stopped at the firm boundary. Today, many wallets intentionally stay closed-loop for competitive reasons. Value does not move easily or cheaply across providers, so customers get locked in and inclusion suffers. The cure is to institutionalise interoperability through open rails, fair access, and clear recourse while enforcing trust primitives like consent, portability, resilience, and redress. That balance lets innovation move fast while value and data move freely and safely – which is how inclusion, consumer protection, and trust are sustained.

Acronyms

A2A: Account-to-Account
AIS / AISP: Account Information Service (Provider)
AML/CFT: Anti-Money Laundering and Countering the Financing of Terrorism
API: Application Programming Interface
CBDCs: Central Bank Digital Currencies
CD: Continuous Development
CI: Continuous Integration
CTO: Chief Technology Officer
FAPI: Financial-grade API
GIZ: Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH
JARM: JWT Secured Authorisation Response Mode
KPIs: Key Performance Indicators
KYB: Know Your Business
KYC: Know Your Customer/Client
LEI: Legal Entity Identifier
MSME: Micro, Small, and Medium Enterprises
mTLS: Mutual Transport Layer Security
NBFIs: Non-Bank Financial Institutions
OBIE: Open Banking Implementation Entity
OIDC: OpenID Connect
PCI DSS 4.0: Payment Card Industry Data Security Standard version 4.0
PEP: Politically Exposed Person
PIS / PISP: Payment Initiation Service (Provider)
PSD2: Payment Services Directive 2
PSP: Payment Service Provider
PTSP: Payment Terminal Service Provider
RESTful API: Representational State Transfer Application Programming Interface
RPO: Recovery Point Objective
RTO: Recovery Time Objective
SLAs: Service Level Agreements
SLOs: Service Level Objectives
TLS: Transport Layer Security
TPP: Third-Party Provider
VASPs: Virtual Asset Service Providers

Elias M. Tayeh

Elias M. Tayeh is a digital finance strategist with over 20 years of international experience leading fintech, regulatory, and digital transformation initiatives across the MENA region, West Africa, and beyond. He is the Founder and General Manager of Cedratech Consulting Services Ltd., a consultancy specialising in digital finance solutions, systems modernisation, and systems integration. He also serves as Managing Director of Epic Payment Technologies Ltd., a licensed Payment Services Provider under the Central Bank of Nigeria. Elias has advised semi-governmental authorities, regulatory authorities and financial institutions on open banking, Digital Finance, RegTech, SupTech, and national payment platforms. His work emphasises and embeds financial inclusion, consumer protection, SME finance, and women-led business empowerment. He has delivered training programmes at the IBS Fintech Academy Jordan, CBF Tunisia, and Alex Bank Egypt, and has collaborated on large-scale projects with GOPA AFC, GFA Group, and the Frankfurt School of Finance & Management. He also recently participated as a session chair and session moderator at the Amman Forum 2025 – “Harnessing Artificial Intelligence in Combating Money Laundering and Terrorism Financing: Opportunities, Risks, and the Way Forward”, held in September 2025 in Amman, Jordan. The forum addressed topics such as artificial intelligence in AML/CFT, supervisory innovation, and the role of RegTech and SupTech in compliance.



34 Lime Street, London EC3M 7AT
www.agrc.org
info@agrc.org