AKURATECO

On-Premises Payment Orchestration

Meeting Local Requirements in the GCC

2026–2027 Edition · September 2026

Contents

Introduction

Two years ago, the question payment companies asked about the Middle East and North Africa was whether to enter. That question is settled. Electronic payments now account for 85% of all retail payments in Saudi Arabia. Qatar's payment ecosystem moved QR106.8 billion in a single month this summer, 40% more than a year earlier. The UAE's instant payment platform has 12.5 million users.

The question now is harder: can you actually operate here?

MENA is not a market. It is a dozen jurisdictions that happen to share a map. There is no MENA licence, no MENA cloud region, no MENA payment method. Each country has its own regulator, its own domestic card scheme, its own instant payment rail, and — increasingly — its own rule about where your transaction data is physically allowed to sit.

Two forces, pulling in opposite directions

Anyone building or scaling a payment institution in the Gulf is being pulled two ways at once.

The regulator pulls you inward. Payment data has to be processed and stored inside the country, on infrastructure you can point to, with a disaster recovery arrangement the supervisor has approved. In the UAE and Qatar this is written into the instruments. In Saudi Arabia it is the practical default.

The market pushes you outward. A merchant in Doha expects to accept the domestic scheme *and* Visa *and* Mastercard *and* Apple Pay *and* Google Pay — settled through whichever of several local acquiring banks offers the best rate and the highest approval rate, with a fallback for when one has a bad hour, and an instant rail alongside all of it.

Satisfy only the first and you have a compliant platform nobody wants to use. Satisfy only the second and you cannot get licensed.

> There is exactly one component where both are satisfied at the same time: **the payment orchestration layer, deployed inside the jurisdiction.** An orchestration platform is what lets a single institution reach every rail its market expects. Running it on dedicated in-country infrastructure is what keeps the regulated data — card numbers, tokens, cardholder details, the complete transaction record — inside the border the regulator drew. Neither half works without the other.

This edition sets out what that requires in practice: the licensing reality market by market, the residency rules that decide your architecture, what the orchestration layer does and why it has to run locally, and what we have learned deploying it in the region ourselves.

What has changed since our last edition

- **MENA stopped being an emerging market.** Saudi Arabia passed its 2025 cashless target and kept going.
- **Localisation moved from preference to licence condition.** The UAE and Qatar now impose explicit, instrument-level requirements on where payment data lives. Saudi Arabia's position is more nuanced than most commentary suggests.
- **Account-to-account is taking value share from cards.** In Qatar's July 2026 figures, card payment *value* fell 11% year on year while total ecosystem value rose 40%. Reaching the new rails is an orchestration problem.
- **PCI DSS has no runway left.** All 51 future-dated v4.x requirements became mandatory on 31 March 2025.
- **The cloud map filled in.** Saudi Arabia and Qatar now have live hyperscaler regions, with two further Saudi regions scheduled before the end of 2026.

PART ONE

The 2026 Market Picture

Saudi Arabia has already won its cashless argument

Electronic payments reached **85% of total retail payments in 2025**, up from 79% in 2024 and 36% in 2019, across **14.6 billion transactions** — up from 12.6 billion the year before. The Financial Sector Development Program target of 70% by 2025 was passed well ahead of schedule. There were 301 fintech companies operating in the Kingdom at the end of 2025 against a Vision 2030 target of 525, and payments firms make up 28.2% of them.

85%
Share of Saudi retail payments made electronically in 2025, up from 79% in 2024 — SAMA

14.6bn
Saudi electronic payment transactions in 2025, up from 12.6bn — SAMA

QR106.8bn
Qatar's payment ecosystem value in July 2026, up 40% year on year — QCB

12.5m
Users on the UAE's Aani instant payment platform by April 2026 — CBUAE

Qatar is growing fast, but not how most people assume

In July 2026 the Qatar Central Bank's payment ecosystem handled **QR106.8 billion across 72.5 million transactions** — value up 40% year on year, volume up 23%. Fawran, the instant rail, more than doubled: QR6.8 billion across 3.9 million transactions, both up 108%, from 3.9 million registered accounts.

Read the composition and the strategic message changes. Account-to-account transfers made up **79% of that total value**, growing 63%. Fawran accounted for a further 6%. Card payments totalled QR22.5 billion — volume up 15%, but **value down 11%**.

The lesson is architectural. Card acquiring alone is a shrinking share of a growing pie. The institutions capturing the growth are connected to the instant and account-to-account rails as well as the card rails — which makes the ability to add a rail quickly worth more than the ability to process a card cheaply.

The UAE has built national infrastructure and put the state behind it

Aani reached **12.5 million users by April 2026** across 74 connected financial institutions, with transfers completing in about three seconds and a sixfold year-on-year increase in transfers. Jaywan, the domestic card scheme, entered its second issuance phase in July 2026, and the world's first co-badged Jaywan–Mastercard credit card was announced the same month. In August 2026 the Ministry of Finance adopted both for federal fees and fines.

Egypt's growth is real and increasingly wallet-led

InstaPay had 16 million users as of November 2025, having processed roughly 1.1 billion transactions worth EGP 2.4 trillion in the first half of 2025. Telco-linked mobile wallets moved **EGP 2.96 trillion in the first half of 2026 alone**, up 56% year on year across 2.22 billion transactions, from 57 million registered wallets.

The opportunity, sized

Measure	2026	2031	CAGR	Source
MENA digital payments	$275.5bn	$462.4bn	10.9%	Mordor Intelligence
MEA e-commerce	$176.7bn	$338.1bn	13.9%	Mordor Intelligence
Saudi e-commerce	$31.3bn	$54.9bn	11.9%	Mordor Intelligence
Middle East BNPL	$3.3bn	$8.8bn	21.3%	Research and Markets

Capital is following, though its shape matters. MENA startups raised **$7.5 billion in 2025** across 647 companies, and fintech took **$4.4 billion — 58% of all funding**. Just over half the total was debt rather than equity. The first half of 2026 was quieter at $1.7 billion, with fintech again leading at $708 million.

BNPL has matured from growth experiment into licensed financial infrastructure. Tabby reached a $4.5 billion valuation in a secondary share sale in October 2025, with over 15 million users and 40,000 merchants across Saudi Arabia, the UAE and Kuwait. Tamara holds a full SAMA consumer finance and BNPL licence. For a payment institution this means BNPL is another rail your merchants' customers expect at checkout, not an optional add-on.

Cloud adoption is mainstream too: 78% of Middle East organisations report medium-to-high cloud maturity and 86% plan to increase investment. The number worth pausing on is that **51% use or plan to adopt sovereign public cloud.** Localisation is not only regulatory pressure. It has become a procurement preference.

> The regulators in MENA aren't just talking about changes — they're pushing for effective execution. Regulators intend not just to make policies but enforce them with speed and precision.
>
> Gaurav Sachddeva, Co-Chair, MENA Fintech Association

Two GCC institutions that went from licence to live traffic

View the case studies →

PART TWO

There Is No MENA Licence

The most expensive mistake in regional expansion is treating MENA as one market with one entry plan. A licence in Qatar tells you nothing about what Saudi Arabia will require.

Regulation here is not the obstacle it is assumed to be. Financial regulators across MENA are broadly pursuing three consistent objectives — fair competition, ecosystem protection, and enabling innovation — and all three favour a well-prepared entrant. What defeats companies is the assumption that one set of rules applies everywhere.

Market	Primary instrument	Categories and minimum capital	Decision timeline
Saudi Arabia	Law of Payments and Payment Services (RD M/26, 2021); PSP Regulations	Major Payment Institution SAR 3m; Micro PI SAR 1m; Major EMI SAR 10m; Micro EMI SAR 2m	No published clock; plan 9–12 months
Qatar	Payment Services Regulations, QCB Circular 23 of 2021	E-money issuance, merchant acquiring, local fund transfer. Capital requirements exist but are unpublished	Not published
UAE onshore	Retail Payment Services and Card Schemes Regulation, C 15/2021	Cat I AED 3m / 1.5m; II AED 2m / 1m; III AED 1m / 500k; IV AED 100k. Higher figure where monthly volume ≥ AED 10m	Not published; plan 6–9 months
UAE — DIFC	DFSA Money Services Business	Base capital Cat 4 $140k; Cat 3D $200k; Cat 3C $500k — see note below	~90–120 business days
UAE — ADGM	FSRA Providing Money Services	Enhanced framework since 2020; base capital not published	3–5 months (indicative)
Egypt	CBE Rules for Licensing PSOs and PSPs, 19 June 2025	PSP Cat A EGP 30m; Cat B EGP 10m; PIS/AIS EGP 20m; System Operator EGP 500m	90 days, extendable once
Bahrain	CBB Rulebook Volume 5, PSP Module, February 2026	BD 30,000–50,000 by service, plus six months' opex in net equity	**60 calendar days** — fastest in the region
Kuwait	CBK Resolution 45/471/2023	Small EPSP KWD 50k; Large EPSP KWD 250k; Small EMSP KWD 100k; Large EMSP KWD 1m; Operator KWD 2m	Initial approval valid six months
Oman	National Payment Systems Law RD 8/2018; Banking Law RD 2/2025	PSP, E-Money Issuer, System Operator	No PSP-specific clock published
Jordan	Electronic Payment and Money Transfer Bylaw 111 of 2017	System Operator; Payment Service Provider	90 days initial; 6 months to fulfil; 90 days final
Morocco	Law 103-12 (*établissement de paiement*)	Payment accounts, transfers, instrument issuance, e-money	Not published

Several figures are not published by the regulator — Qatar, ADGM, Oman, Jordan and Morocco should be confirmed with local counsel before budgeting, and sources conflict on Egypt's System Operator figure. Timelines other than Bahrain's, Egypt's and Jordan's are practitioner estimates.

A note on DIFC. Amendments to the DFSA's prudential rules took effect on 1 July 2026, introducing an Activity-Based Capital Requirement alongside Stored Value and Transaction-Based requirements aimed specifically at money services providers. Firms hold the highest applicable measure. Treat the table as a floor and model the new requirements before committing to DIFC.

Three structural changes worth building into your plan

The UAE has widened its perimeter to reach technology providers. Federal Decree-Law No. 6 of 2025 came into force on 16 September 2025 with a one-year transition ending 16 September 2026. It extends licensing to technology providers that "facilitate or enable" financial services — language that explicitly captures payment gateways, fintech platforms and APIs connecting customers to financial institutions. Fines reach AED 1 billion, with a minimum AED 1 million penalty for unlicensed activity. If your UAE model assumed you were a vendor behind someone else's licence, re-test that assumption.

Qatar has improved payment economics twice in eighteen months. Since May 2025, fintechs integrate **directly with NAPS and QPay**, removing the mandatory bank intermediary. Since 1 September 2026, licensed PSPs may **hold central bank accounts and access QA-RTGS directly**. Both are integration opportunities: they reward whoever connects to a new rail fastest.

Saudi Arabia moved open banking from sandbox to licensed activity. SAMA issued its licensing framework in March 2026 and granted the first licence — to Lean Technologies, as a Major Payment Institution — the same month.

Where should you start?

- **B2C? Population is the first filter.** Saudi Arabia has over 40 million people; Qatar around three million. That decides whether a consumer proposition can reach scale.
- **B2B? Ecosystem access matters more.** Qatar's banks are large and reachable — a small ecosystem is an advantage when you need to get in front of decision-makers.
- **Easiest to enter is the UAE — and hardest to win in.** Unless you bring a distinct proposition or serve an underserved vertical, ease of entry is a poor reason to choose it.
- **Fastest published decision is Bahrain**, at 60 calendar days.

Whichever you choose, the sequencing principle holds: get one market live, then let the second benefit from the template.

PART THREE

Data Residency

Every technical decision in a MENA deployment is downstream of this one. The short version: **the UAE and Qatar impose hard, explicit, instrument-level localisation. Saudi Arabia's position is more nuanced than commonly reported and changed materially in 2024–2025. Egypt has no localisation statute but reaches a similar outcome by another route.** Plan for separate in-country deployments per market.

United Arab Emirates — the clearest requirement in the region

Two independent instruments each require in-country storage. **Article 14(22)** of the Retail Payment Services and Card Schemes Regulation states that personal and payment data "shall be stored and maintained in the State," with a secure backup in a separate location for five years. **Article 6.1.6.3** of the Consumer Protection Standards separately requires all licensed financial institutions to "hold and store all Consumer and transaction Data within the UAE."

For banks, **Article 6 of the Outsourcing Regulation** sets the offshore gate: data leaving the country requires *both* prior CBUAE approval *and* prior written customer consent, including acknowledgement that data may be accessed in foreign legal proceedings. That instrument addresses banks rather than PSPs, but it is the clearest published statement of how the Central Bank thinks, and PSPs should expect their licence conditions read against it.

DIFC and ADGM apply GDPR-style transfer mechanics instead and carry no CBUAE localisation mandate — but a free zone licence does not give you the onshore retail market either.

Design conclusion: UAE-resident primary and UAE-resident backup.

Qatar — in-country primary, QCB authorisation for anything else

The QCB **Data Handling and Protection Regulation** of February 2025 applies to all financial institutions under QCB supervision and is unusually direct.

- **Section 7.6** requires the primary environment — the main data storage and processing environment — for personally identifiable, sensitive personal and **sensitive financial information** to reside within the State of Qatar.
- **Section 7.7** requires explicit QCB approval *before implementation* of any foreign storage.
- **Section 15.1** prohibits international transfer of any of those categories without QCB authorisation, with 15.2–15.6 setting out mandatory pre-transfer due diligence.
- **Section 18.2** makes the QCB Cloud Computing Regulation (April 2024) mandatory as a secondary regulation.

The implication is frequently missed: a data processing agreement plus standard contractual clauses is **not** sufficient in Qatar. You need affirmative, prior, explicit QCB approval, on two separate grounds.

Saudi Arabia — more nuanced than the market believes

Most published commentary is out of date. There are four layers, and the strictest was removed.

Personal data transfers. The PDPL became fully enforceable on 14 September 2024. SDAIA's revised Data Transfer Regulations established three safeguard routes — standard contractual clauses, binding common rules, and a certificate of accreditation. The adequacy list has not been published, so appropriate safeguards remain the operative route. On the face of these instruments, cross-border transfer of personal data is **permitted with conditions** rather than prohibited, though some official commentary describes a broader requirement to keep sensitive and personally identifiable data in the Kingdom, and the two readings have not been publicly reconciled.

The cloud controls that were removed. The National Cybersecurity Authority's CCC-1:2020 contained two provider controls requiring cloud services to be delivered from within the Kingdom: one covering storage, processing and disaster recovery centres, the other monitoring and support. Per the NCA's published change log for **CCC-2:2024**, both were removed and the localisation obligation transferred to the National Data Management Office at SDAIA. This is one of the most commonly mis-reported points in the region — though the Arabic text is binding and should be confirmed before an architecture depends on it. Removal does not mean the obligation disappeared. It moved.

SAMA's own rule, which is what binds a payment institution. Section 3.4.3 of the SAMA Cyber Security Framework (v1.0, May 2017) states that "in principle only cloud services should be used that are located in Saudi

Arabia, or when cloud services are to be used outside Saudi Arabia that the Member Organization should obtain explicit approval from SAMA."

What the market is doing. Mastercard moved processing on-soil in October 2024 and was certified for SAMA's E-commerce Payments Interface in December 2025. Visa launched a locally hosted Acceptance Platform in September 2025, citing SAMA's in-Kingdom hosting expectation directly.

Design conclusion: in-Kingdom hosting is the practical default. It is not an absolute prohibition on offshore processing — but treat that as a bespoke regulatory negotiation, not a compliance checkbox.

Egypt — no statute, similar outcome

Egypt has no general localisation requirement in the PDPL or its Executive Regulations, issued 1 November 2025. But two things produce the effect anyway: outsourcing providers must be registered with the Central Bank of Egypt, which does not generally accept companies established outside Egypt; and the June 2025 licensing rules require a PSP to be an **Egyptian joint stock company exclusively dedicated to payment services**. Note too that CBE-regulated entities other than money transfer companies are excluded from the PDPL entirely, falling under Banking Law 194 of 2020 instead.

The disaster recovery myth worth correcting

It is widely assumed that SAMA requires a Saudi institution's disaster recovery site to be inside Saudi Arabia. **The SAMA Business Continuity Management Framework does not say that.** It requires an alternative data centre "at an appropriate location," selected through a risk assessment ensuring it does not share the same risks as the main site. There is no residency mandate, no minimum distance, and no RTO/RPO tier grid.

There *is* a requirement people routinely miss: **SAMA approval is required when selecting or relocating either the main or the alternate site.** The in-Kingdom pressure on a Saudi DR site comes from the cloud rule, not the continuity rule.

Where the clouds actually are

Residency requirements are only satisfiable where a compliant region exists.

Market	Live hyperscaler regions	Scheduled
Saudi Arabia	Google Cloud (Dammam, 2023); Oracle Cloud (Jeddah 2020, Riyadh 2024)	AWS — December 2026; Microsoft Azure — Q4 2026
Qatar	Microsoft Azure (Doha, 2022); Google Cloud (Doha, 2023)	—
UAE	Microsoft Azure (Dubai, Abu Dhabi, 2019); AWS (2022); Oracle Cloud (Dubai, Abu Dhabi)	—
Bahrain	AWS (2019)	—
Egypt	None	—

Three things follow. Any claim that all major hyperscalers are live in Saudi Arabia is incorrect today, though it should be close to true by early 2027 — announced dates are targets and do slip. Egypt has no hyperscaler region at all, which makes the CBE's preference for locally established providers a harder constraint than it first appears. And if your architecture assumes a specific provider, check it has a region in the country your licence requires *before* you commit.

Every market in that table needs its own in-country deployment

Explore on-premises deployment →

PART FOUR

The Orchestration Layer

Part Three set out what the regulator requires. This part sets out what the market requires — and why the two meet in a single piece of software.

What a payment orchestration platform actually is

The term is used loosely. A gateway is one connection: it takes a transaction and sends it somewhere. An orchestration platform decides *where*, *in what order*, and *what to do when that fails*. Concretely, six things:

- **A connector layer** — normalised, pre-built integrations to acquiring banks, domestic card schemes, instant payment rails, wallets, alternative payment methods, BNPL providers, anti-fraud and KYC/KYB providers, behind one API.
- **A routing engine** — configurable rules deciding, transaction by transaction, which connection to use: by BIN, scheme, currency, amount, merchant, MCC, issuer country, cost or time of day.
- **Cascading and retry logic** — when the first attempt declines or times out, the next route is attempted automatically, before the customer abandons checkout.
- **A token vault** — card data stored once, centrally, reusable across every connected acquirer, so changing a route does not lose the customer's saved card.
- **Merchant management** — onboarding, configuration, limits, fee structures, sub-merchant hierarchies.
- **Reconciliation, settlement and reporting** — one authoritative record of what was authorised, captured, settled, and owed.

The distinction that decides whether you need one: a gateway answers *can this transaction be processed?* An orchestration platform answers *what is the best way to process it, and what happens if that route is unavailable?*

Why the GCC forces plurality

In some markets a single acquirer relationship is a viable business. In the Gulf it is not, because the rails a merchant expects do not come from one place.

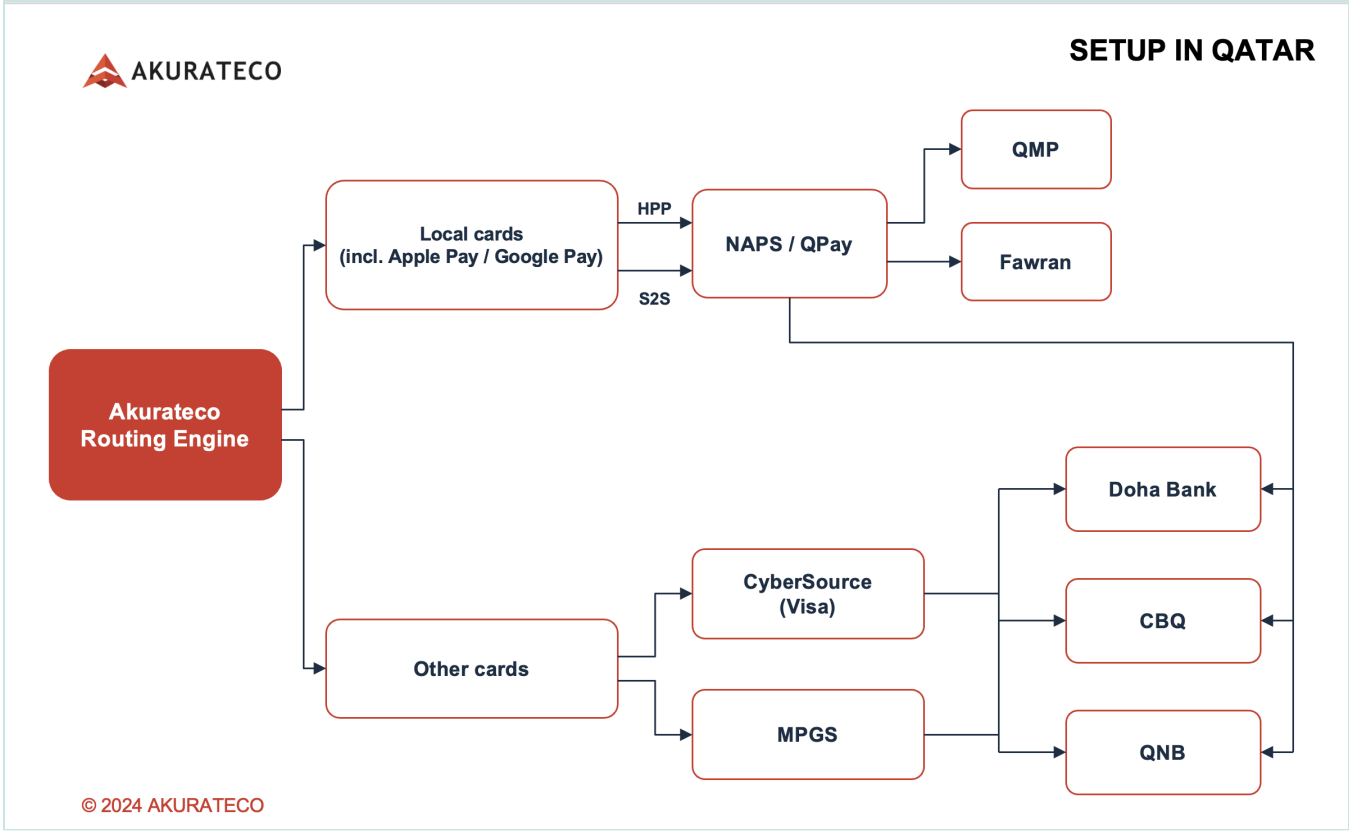
Market	Domestic card scheme	Instant / A2A rail	International	Wallets	BNPL
Saudi Arabia	mada — effectively mandatory for domestic card acceptance	sarie	Visa, Mastercard via SAMA-certified gateways	Apple Pay, Google Pay	Tabby, Tamara
Qatar	NAPS / QPay	Fawran; QMP wallets	Visa, Mastercard	Apple Pay, Google Pay	PayLater, Tamanna
UAE	Jaywan	Aani	Visa, Mastercard	Apple Pay, Google Pay	Tabby, Tamara, others
Egypt	Meeza	InstaPay — non-bank access needs a bank sponsor	Visa, Mastercard	Local wallets	Growing

Each column is a distinct technical integration with its own protocol, certification process and settlement cycle. The domestic scheme is not a variation on Visa; it is a separate rail. The instant payment system is not a card transaction; it is a different message format entirely.

Then layer the commercial requirement on top. You need **at least two acquiring partners** per market — for rate arbitrage, for approval-rate optimisation, and above all so that one acquirer's outage is not your outage. That is a minimum of five or six live integrations per market, each with a routing decision attached, before you have written a line of your own product.

Anatomy of a live GCC deployment

The diagram below is the actual routing topology of **TESS Payments**, a Qatar Central Bank-licensed payment service provider running on Akurateco's platform. It is what the previous two pages look like when they are built.



The routing topology of a Qatar Central Bank-licensed payment institution: one engine splitting local and international card traffic across NAPS/QPay, QMP, Fawran, CyberSource, MPGS and three acquiring banks.

Everything enters at the routing engine. The first decision is card origin.

Local cards, including Apple Pay and Google Pay, route to NAPS/QPay, Qatar's domestic switch, over two flows — a hosted payment page for merchants who want the card form out of their PCI scope, and server-to-server for merchants keeping checkout inside their own application. From there the transaction reaches **QMP**, the mobile payment scheme, or **Fawran**, the instant payment rail, with settlement running back to the acquiring banks.

Everything else takes the international path: **CyberSource** for Visa and **MPGS** for Mastercard, each landing in one of three acquiring banks — **Doha Bank, Commercial Bank of Qatar and QNB**.

Four things are worth naming.

The domestic and international schemes are separate rails, not variants of one. Different protocols, certifications and settlement. Supporting both means integrating both, and keeping both current as each evolves.

Three acquirers, not one. That is what makes routing rules and cascading meaningful — and what turns an acquirer's bad hour into a rerouted transaction rather than a lost one.

Wallets are a form factor, not a payment method. Apple Pay and Google Pay ride the local card rail, which is precisely why network tokenisation has to live in the orchestration layer rather than at the edge.

This is not a gateway with a Qatari address. It is a Qatari payment topology — and it exists only because something in the middle knows how to route into it, and can be reconfigured when the topology changes.

The point this builds to

Look at the diagram again and ask a different question: where is the sensitive data?

Every routing decision in that picture is made by software that is, at that moment, holding the card number or its token, the cardholder's personal data, and the complete transaction record. The token vault sits behind the routing engine. The reconciliation record is assembled there. The fraud decision is taken there.

Which is to say: **the orchestration layer is where all the data the regulator cares about is concentrated.**

The full TESS Payments build, including the migration architecture

Read the case study →

PART FIVE

Why It Has to Run Inside the Jurisdiction

What the orchestration layer actually holds

Set the terminology aside and list what the platform processes and stores:

- Primary account numbers and network tokens, in the vault
- Cardholder personal data — name, contact details, billing address, device and session data
- The complete transaction record — amount, merchant, timestamp, result, decline reason
- Routing and settlement data
- Fraud signals and the decisions taken on them

Compare that against Part Three. It is every category named in **Article 14(22)** of the UAE's Retail Payment Services regulation. It is every category named in **sections 7.6 and 15.1** of Qatar's Data Handling and Protection Regulation, including sensitive financial information. It is exactly what SAMA's cloud rule points at.

The orchestration layer is not an adjacent system that happens to touch regulated data. It *is* the regulated data, in motion and at rest.

Why the standard SaaS model does not solve this in the Gulf

Most payment orchestration platforms are multi-tenant SaaS processing in a handful of global regions — Frankfurt, Ireland, Northern Virginia. That model is excellent nearly everywhere in the world. It is fast to adopt, upgrades itself, and spreads cost across a large tenant base.

In the GCC it puts the regulated data outside the jurisdiction by design, and no contract fixes that. Qatar requires prior QCB authorisation for the transfer and separate approval for foreign storage. The UAE requires in-country storage as a baseline, with CBUAE approval *plus* per-customer consent to move anything offshore.

This is the position institutions find themselves in: the platform with the connector breadth they need cannot be deployed where their licence requires, and the platform they could deploy locally does not have the connectors. So they start building — and Part Seven describes what that costs.

The third option

There is a third model, and it is the one this whitepaper argues for: **an orchestration platform deployed as dedicated, single-tenant infrastructure inside the country.**

A word on terminology. When we say **on-premises**, we mean a dedicated, single-tenant deployment in an environment controlled by the institution — whether a physical data centre or a dedicated cloud tenancy in a specific country. The contrast is with multi-tenant SaaS, not with cloud infrastructure. In practice, most GCC deployments today are dedicated tenancies in an in-country hyperscaler region.

What that gives you is the connector breadth, routing engine and token vault of a mature global platform, with the data residency of a local build.

	Multi-tenant SaaS	Dedicated in-country	Build in-house
Time to first transaction	Weeks	Weeks to a few months	2–3 years
Residency in UAE / Qatar	Not satisfied without regulator approval	Satisfied by design	Satisfied by design
Connectors live on day one	Full catalogue	Full catalogue	None
Control over routing logic	Configurable within vendor limits	Yours, on your infrastructure	Total
Evidence for the regulator	Vendor attestation	You can show the components	You can show the components
Ongoing cost profile	Lowest	Moderate	Highest

Four benefits that are not compliance tick-boxes

Evidence, not assertion. A supervisor asking how failover works, where the token vault sits, or which components hold cardholder data wants to be shown, not told. A dedicated in-country deployment means every answer is a diagram of your own infrastructure. This matters most in Saudi Arabia, where SAMA approval is required for site selection and the security control set applies to the DR site as well as production.

The routing logic is yours. Rules, cascading order, acquirer priorities and cost logic are configured by you, running on your infrastructure, and changed when you decide — not when a vendor's release train reaches you.

No dependency on someone else's roadmap. When QCB opened direct NAPS and QPay integration in May 2025, and direct QA-RTGS access in September 2026, the institutions that captured the economics were those who could integrate on their own schedule. The same will be true of SAMA's E-commerce Payments Interface and of Jaywan and Aani. A rail opening is a race, and being one queue-position in a shared vendor backlog is how you lose it.

Sovereignty over the token vault. Card data stored inside the jurisdiction, under your control, is both a regulatory position and a commercial one — it is what makes adding an acquirer a configuration change rather than a re-tokenisation project.

And one honest caveat

Dedicated in-country deployment is not right everywhere. One heavily regulated market rewards it. Fifteen lightly regulated markets punish it — you would run fifteen environments to solve a problem two of them actually have. The rule: **deploy locally where a regulator requires local, and use shared infrastructure where none does.** In the GCC, that means locally.

PART SIX

The Rest of the Stack

A licence is permission to operate; the orchestration layer is the machinery. Everything else that has to be live:

- **The local entity.** In several markets the structure is prescribed — Egypt requires a joint stock company dedicated exclusively to payment services.
- **Local infrastructure and PCI DSS.** Hard requirements in the UAE and Qatar, the practical default in Saudi Arabia and Egypt. This is the long pole; it starts before you need it.
- **Acquiring relationships** — at least two per market.
- **Domestic schemes and rails.** In Saudi Arabia, SAMA's E-commerce Payments Interface (July 2025) sets unified technical specifications requiring local routing, tokenisation, fraud prevention and direct mada integration; no compliance deadline has been published, but the certification wave through late 2025 and early 2026 suggests real pressure. In Egypt, non-bank access to the Instant Payment Network is restricted to banks, so you need a bank sponsor for InstaPay today.
- **Wallets and tokenisation.** Apple Pay and Google Pay are baseline expectations. Network tokenisation is a revenue feature rather than a compliance one: it improves authorisation outcomes, and it requires infrastructure you control.
- **Anti-fraud**, orchestrated alongside the routing decision, configured to the merchant's vertical — fraud patterns in travel, marketplaces and digital goods have almost nothing in common.
- **Billing, reconciliation and settlement.** Unglamorous and consistently underestimated. Daily, not monthly.

PCI DSS — and a point most institutions are still missing

PCI DSS v4.0.1 is the current and only accepted version, and all 51 future-dated requirements from v4.0 became mandatory on **31 March 2025**. There is no remaining runway.

Two requirements deserve attention because they apply to you as a service provider, not only to your merchants. **Requirements 6.4.3 and 11.6.1** require payment page scripts to be authorised, integrity-checked and monitored for tampering. The Council has confirmed applicability extends to payment processors providing embedded iframes.

Under **FAQ 1588**, effective 1 April 2025, e-commerce merchants using embedded payment forms can only remain on SAQ A if they either implement script protections themselves **or obtain written confirmation from their PCI DSS-compliant service provider that the embedded solution includes them.**

Being able to issue that confirmation is now a competitive requirement in SMB acquiring. An institution that cannot will lose small-merchant business to one that can.

PART SEVEN

Build, Buy or Co-Build

The sequencing trap

The instinctive answer for a well-funded institution is to build. Own the stack, own the roadmap, own the margin.

In practice, building a compliant orchestration platform from scratch typically takes two to three years before a single live transaction — and that is before onboarding local acquirers, certifying with the domestic scheme and passing PCI DSS. In a market growing at double digits annually, a three-year build is not a technology decision. It is a decision to arrive late.

There is also a circularity that catches first-time entrants. You need demonstrated technical capability to satisfy the regulator before you get a licence. But you cannot easily justify dedicated in-country infrastructure before you have the licence. Institutions planning for a single deployment event get stuck in that loop.

The way through is to treat deployment as two phases: launch on a certified, connector-rich platform fast enough to support the licensing process, then migrate to dedicated in-country infrastructure once licensed, with transaction synchronisation across both environments so the migration is invisible to merchants. In several MENA markets it is the only order that works.

The four questions that decide it

1. **Does your licence require local infrastructure?** In Qatar and Saudi Arabia, a domestic licence effectively mandates it. As an agent or reseller under someone else's licence, it may not.
2. **How many markets are you serving?** One heavily regulated market rewards dedicated deployment. Fifteen punish it.
3. **What is your sequencing constraint?** If you need demonstrated capability to obtain a licence, SaaS first and dedicated second is the answer.
4. **Who owns the migration risk?** Moving to dedicated infrastructure after you have live merchants is the highest-risk moment in the business. Plan it before launch, with dual-running and transaction synchronisation, not afterwards.

What merchants are actually buying

The overwhelming majority of merchants care very little about your infrastructure. What they care about is reliability, credibility, speed, support and brand trust. A young payment institution competing head-to-head with a national bank does not win on architecture diagrams. It wins by answering the phone.

But those five things are all *outputs* of orchestration and infrastructure decisions. Uptime is an architecture decision. Approval rate is a routing and tokenisation decision. Whether a declined transaction is retried on a second acquirer or simply lost is a cascading decision. How fast you can add an acquirer when a merchant asks is a connector-layer decision. Whether you survive a regional outage is a disaster recovery decision.

Your merchants will never ask about any of that. They will simply leave if you get it wrong.

> Merchants are looking for a single API solution that connects them to all acquiring banks and local payment methods seamlessly. This integration layer is key to enabling global aspirations.
>
> Gaurav Sachddeva, Co-Chair, MENA Fintech Association

PART EIGHT

Deploying the Orchestration Layer In-Country

This section is deliberately more technical. It sets out how Akurateco actually deploys the platform inside the region: which clouds, which architecture, how disaster recovery is structured, and what we ran into. Client names are withheld throughout.

Where we run

We operate live, in-country deployments across three cloud platforms in the region: **Microsoft Azure in Qatar**, with disaster recovery in a European region; **Oracle Cloud Infrastructure in Saudi Arabia**, with in-Kingdom disaster recovery designed to SAMA requirements; and **Google Cloud in Saudi Arabia** — alongside our own bare-metal data centres and a multi-tenant SaaS platform.

Between them these cover every hyperscaler with a live region in Saudi Arabia or Qatar today. We also run production deployments on **AWS in Europe**. AWS has no Qatar region and its Saudi region is scheduled for December 2026; when it lands, the same architecture is portable to it, adapted to SAMA requirements.

That portability is the substantive claim. It is not that our platform runs on one cloud very well. It is that the same orchestration platform, with the same operational model, runs on four different substrates — three hyperscalers and bare metal — so the choice between them can be made on regulatory and commercial grounds rather than technical ones.

Why Kubernetes, everywhere

Our microservices are containerised, so every deployment uses container infrastructure. The question is only what orchestrates them. In practice that is **Kubernetes**, on every setup, for redundancy and horizontal scaling. Every major cloud provides a managed Kubernetes engine and we use it where one exists. Where one does not — bare metal, or a platform without a managed engine — we stand up our own cluster on virtual machines, exactly as we run our own data centres.

Two clarifications that come up in technical due diligence. We have run microservices directly on a Docker engine on virtual machines, but only as a temporary arrangement during a migration window; it is not a target architecture. And small setups *can* run without Kubernetes — we do not do it, because maintaining two deployment models costs more than it saves.

The consequence for a CTO evaluating us: **the deployment target does not change the platform.** Your team learns one operational model, whether you are on Azure in Doha, Oracle in Riyadh, or bare metal.

How each component is realised

The governing principle: **where the cloud offers a managed service that meets the requirement, we consume it. Where it does not, we deploy the component on virtual machines using the same build we run on bare metal.** That is what makes the platform genuinely cloud-agnostic rather than nominally so.

Component	Managed service where available	Self-managed fallback
Container orchestration	Managed Kubernetes engine (AKS / OKE / GKE)	Self-hosted Kubernetes on VMs or bare metal
Relational database	Managed MySQL-compatible service	**Percona** cluster on VMs, internal replication plus master-master to DR
Search and log analytics	Managed OpenSearch-compatible service	OpenSearch cluster on VMs
Message broker	Managed broker service	RabbitMQ on VMs
Cache	Managed Redis-compatible service	Redis on VMs
Web application firewall	Cloud-native WAF	Virtual NGFW appliance
Secrets management	Cloud-native key/secret vault	Self-hosted secrets manager

Component	Managed service where available	Self-managed fallback
Object storage	Cloud-native object storage	Self-hosted object storage
Monitoring and observability	Cloud-native monitoring, supplemented	Self-hosted monitoring stack
Security monitoring / SOC	—	**Wazuh / ELK** centralised log collection and correlation
DR orchestration	Cloud-native replication and failover tooling	Custom replication and failover procedures
HSM / key management	Cloud-native dedicated HSM offering	Dedicated hardware or virtual HSM

Where it is only a name, and where the mechanics differ

Most of that list is the same capability under a different brand. Object storage is object storage. A message broker is a message broker. Moving between clouds changes the API and the invoice, not the design.

The relational database is where the difference is real — and it is a question of control, not features. It also happens to be where the transaction record and the token vault live, which is why it draws disproportionate attention from supervisors.

With a managed database you provision an instance, configure cross-region replication to your DR site, and you do not see under the hood. It is fast to stand up. In exchange you inherit the provider's failover semantics and cannot intervene in them. When we deploy Percona ourselves we build the same thing explicitly: internal replication for per-node redundancy within the site, and master-master replication to the DR site. It is more work. What you get is a failover path you can inspect, explain and evidence — which matters a great deal when a regulator asks you to demonstrate exactly how recovery works.

The rule we apply: **take the managed service where it meets the requirement; build it where it does not, or where you need to prove how it behaves.**

Three disaster recovery patterns

Which pattern applies to you is decided by your regulator before it is decided by your engineers.

In-country primary, cross-border DR. Our Qatar deployment on Azure runs production in-country with disaster recovery in a European region. The non-obvious part is not the replication. Qatar's Data Handling and Protection Regulation puts the primary processing environment inside Qatar and makes *any* international transfer of personally identifiable, sensitive personal or sensitive financial information subject to prior QCB authorisation. A cross-border DR leg is therefore a regulated arrangement, not a replication job. Data classification, encryption, key residency and the authorisation itself all have to be designed before the first byte replicates. The engineering questions — asynchronous replication latency, and whether failover is automatic or a deliberate documented decision — come second.

In-country primary, in-country DR. For Saudi deployments on Oracle Cloud Infrastructure, disaster recovery sits inside the Kingdom.

Mirror or minimised standby. A DR site can be a full mirror of production or a reduced-footprint standby sized to carry traffic through an unforeseen event or a maintenance window. This is a cost-versus-recovery-time decision worth making explicitly rather than defaulting to a mirror.

Building a Saudi DR site to SAMA expectations

Saudi Arabia is the most demanding environment we deploy into, and the demands are not primarily about the database. The SAMA Cyber Security Framework asks for a control set that, taken together, defines the shape of the site:

- **Identity and access management** on a need-to-know, need-to-have basis, with multi-factor authentication for remote access and, on a risk-assessed basis, for privileged access to critical systems.
- **DDoS protection** including scrubbing services, with 24×7 monitoring and scrubbing tested at least twice a year. The framework is explicit that this applies to the disaster recovery site as well as the main data centre — easy to miss when budgeting.
- **IDS and IPS**, plus deep packet inspection at network level.
- **Network segmentation**, application whitelisting and advanced persistent threat protection.
- **A 24×7 Security Operations Centre** with centralised, automated log analysis and event correlation. We build this on **Wazuh and ELK**.

And the requirement most often overlooked: **SAMA approval is required when selecting or relocating either the main or the alternate site.** That is a gate on your

project plan, not a document you file afterwards.

The network layer is where it gets non-obvious

In our experience, perimeter enforcement on Oracle Cloud Infrastructure cannot rest on native network controls alone. BGP control traffic goes directly to the **Dynamic Routing Gateway** and is not governed by the platform's basic security lists. That gap is what pushes the design toward a full next-generation firewall rather than cloud-native access control lists.

We evaluated four options: **FortiGate, OCI's native firewall, Palo Alto and Juniper SRX.** We selected the **Juniper SRX virtual firewall** on three grounds — L3 through L7 inspection with IPS and advanced threat protection in a single enforcement point; support for make-before-break routing migration, which matters when cutting a live payment environment over without a maintenance window long enough to hide a mistake; and cost, materially better than the alternatives at the same functional level, which is not minor when the same architecture has to be replicated at the DR site.

What we describe here is what the requirements are and what we encountered meeting them. Every Saudi deployment surfaces something the previous one did not.

What we have learned about each cloud

No cloud is best. The observations below are our own, from our own deployments.

Microsoft Azure has given us the strongest scalability and the best support of the three we run in the region. It has also shown operational characteristics we cannot influence: periodic loss of network connectivity between system components, and a heavy Kubernetes upgrade path where upgrades have frequently required manual intervention. We have not found a managed non-relational data store in the shape our platform needs, so that component runs on virtual machines.

Oracle Cloud Infrastructure was the inverse in one respect: the non-relational store worked out of the box, while the relational database did not, so we run Percona ourselves. In Saudi Arabia it has been the strongest option on the two criteria that matter most there — region availability since 2020, and regulatory alignment.

Google Cloud has given us the best automation experience of the three. Our GCP environment came up under Terraform faster and more cleanly than either Azure or Oracle.

AWS, in our European deployments, offers the best fit between our architecture and the managed services available, making it the least expensive for us to install and operate. It is not yet an option in Saudi Arabia or Qatar.

The conclusion we would offer a CTO: there is no best cloud. There is the cloud that has a live region in the country your licence requires, and among those, the one whose managed services align with your architecture. Everything else is a preference.

The same architecture, deployed to SAMA requirements in Saudi Arabia

Read the DineroPay case study →

PART NINE

Scaling, and What Comes Next

Deeper in one market

More merchants and more transactions mean infrastructure has to grow with you: more capacity, more disaster recovery, more availability headroom. This is where service levels start to matter more than features — and where orchestration begins paying for itself measurably. At low volume, a declined transaction is an annoyance. At scale, the difference between a cascading rule that recovers 2% of declines and no cascading at all is a line item on your merchants' P&L, and the reason they stay.

Wider across markets

Every new market repeats the sequence: licence, local setup, PCI DSS, local acquirers, local rails. It compresses the second time because you have a template, but it does not disappear. What gets easier is commercial: merchants you already serve may be targeting the same markets, and their volumes shorten the conversation with a new acquiring bank considerably.

Partnership as a growth channel

The fastest expansion route in this region is usually not a new licence but embedding into an institution that already operates across borders. Telcos deserve particular attention — STC in Saudi Arabia, Ooredoo in Qatar, du and e& in the UAE all operate in multiple jurisdictions with active fintech agendas. Once your solution is embedded with one of them in one market, travelling with them into the next is significantly easier than starting cold.

There is a structural reason these opportunities exist. In Qatar, for example, regulated local banks submit multi-year digital transformation strategies to the central bank, which means the regulator holds an aggregated view of where every institution intends to innovate. Proof-of-concept opportunities surface from that pipeline faster than most fintechs expect.

Across companies we have watched enter MENA successfully, three approaches recur: foreign direct investment, which regulators in healthier jurisdictions prioritise least; know-how transfer, considerably more persuasive because it aligns with what the regulatory framework is trying to achieve; and technology localisation — know-how transfer plus in-country deployment, the combination that shortens the path to being regulated.

What is coming

AFAQ, the GCC's cross-border payment system, reached full central bank participation on **7 September 2026** when the Qatar Central Bank joined, with 74 participating commercial banks across the six states. It is a bank-to-bank corridor rather than a retail rail, so it does not change a payment institution's product today — but it is the infrastructure any future regional retail scheme would be built on. When that scheme arrives, it will be one more rail to integrate, on a deadline set by someone else.

PART TEN

In Practice

Qatar — get licensed first, then move the walls

TESS Payments is a Qatar-headquartered payment service provider, licensed under direct Qatar Central Bank oversight, serving clients including Doha Bank, QNB, Qatar Development Bank and Qatar Fintech Hub. Their obstacle was sequencing: they needed to demonstrate technical and operational capacity to the regulator before a licence, but needed the licence before they could justify dedicated local infrastructure.

We solved it in two phases. TESS launched on our white-label SaaS platform, which gave them a working, certified, connector-rich orchestration layer fast enough to support both their QCB licensing process and their PCI DSS certification. The platform then migrates to dedicated infrastructure on Microsoft Azure inside Qatar, with transactions synchronised across both environments so the cutover is invisible to merchants.

The routing topology that resulted is the diagram in Part Four — a single Qatari institution reaching the domestic switch, the mobile payment scheme, the instant payment rail and three acquiring banks across two international scheme gateways, from one platform, configured once, running inside Qatar.

Saudi Arabia — dedicated infrastructure from day one

DineroPay, a licensed PSP in Saudi Arabia, faced the same residency requirement from a different starting position and made the opposite call. Rather than a phased migration, we deployed dedicated, single-tenant infrastructure immediately on Oracle Cloud Infrastructure, configured to SAMA's requirements for local data storage and encryption, and achieved SAMA certification on that footing.

The reason was market-specific. Saudi mobile payment demand is not a future trend to plan for; it is the present. DineroPay needed Apple Pay and Google Pay live with proper network tokenisation, and the BNPL methods Saudi consumers expect — Tabby and Tamara — alongside cards. Every one of those is a separate connector, and building that stack natively would have consumed the exact window in which the market was being divided up. Read the full DineroPay case study.

A different footprint, a different model

MontyPay, a global payment service provider based in the United Kingdom and part of the Monty Mobile telecommunications group, chose Akurateco's SaaS platform for flexibility, scalability and rapid deployment. MontyPay now operates across MENA, Africa and Asia with over 15 integrations to local and global payment methods — a different deployment model from the two above, chosen because their footprint is many markets rather than one heavily regulated one.

How Akurateco Helps

Akurateco provides a white-label payment orchestration platform that payment institutions and banks deploy under their own brand — as SaaS, as dedicated in-country infrastructure, or as a phased path from one to the other.

- **The orchestration layer, deployable where your licence requires.** The same routing engine, connector catalogue and token vault, running either on our multi-tenant platform or as a dedicated single-tenant deployment inside your jurisdiction. That choice becomes a regulatory and commercial decision, not a technical constraint.
- **Proven regional deployment.** Live, in-country deployments in Qatar and Saudi Arabia across Microsoft Azure, Oracle Cloud Infrastructure and Google Cloud, plus our own bare-metal data centres and production AWS deployments in Europe. Our clients operate under licences from regulators including SAMA, the Qatar Central Bank and Egypt's Financial Regulatory Authority.
- **700+ pre-integrated connectors** across 200+ currencies — acquiring banks, domestic schemes, local payment methods, wallets, anti-fraud and KYC/KYB providers, through a single API.
- **Intelligent routing and cascading**, merchant onboarding, tokenisation, analytics and risk management, configurable by your team rather than ours.
- **PCI DSS Level 1 certified** across the hosted components, including the hosted payment page, tokenisation and card data storage — which is what lets your merchants stay on the lightest applicable SAQ.
- **A clear division of responsibility.** The licence and the acquiring agreements are yours, in your name. We supply the technology and help you connect the right acquiring partners.

Final Thoughts

Localisation looks like a cost when you are outside the market. From inside it, it is the most durable competitive advantage available — because the same requirement that slowed you down is now keeping your competitors out.

But localisation alone is only half a strategy. An institution that satisfies the regulator and can reach one acquirer has built a compliant business with no commercial edge. An institution that can reach every rail its market expects, but has to process the data abroad to do it, cannot get licensed at all.

The institutions that will own GCC payments over the next five years are the ones that put the orchestration layer — the routing engine, the connector catalogue, the token vault, the transaction record — inside the border the regulator drew, and then used it to move faster than everyone still waiting on a vendor's release schedule.

The region is not waiting. Saudi Arabia passed its 2025 cashless target and kept climbing. Qatar's payment value grew 40% in a year and opened two new rails in eighteen months. The licences are being issued now.

Everything in this document is solvable. None of it is solvable quickly if you start late.

See the platform running the deployments described here

Request a demo →

Appendix: Sources

Market data. Saudi Central Bank (SAMA), electronic payments statistics FY2025, published 12 April 2026 · Qatar Central Bank monthly payment ecosystem data, July 2026; QCB Annual Report 2025 · AI Etihad Payments / Central Bank of the UAE, Aani press release, 10 April 2026; CBUAE Financial Stability Report 2025 · Central Bank of Egypt data presented at PAFIX 2025, November 2025; NTRA mobile wallet data, H1 2026 · Mordor Intelligence, *MENA Digital Payments Market*, *Middle East and Africa E-commerce Market* and *Saudi Arabia E-commerce Market*, 2026 · Research and Markets, *Middle East Buy Now Pay Later Business Report 2026* · Wamda, MENA startup funding reports, January and July 2026 · Fintech Saudi, annual review 2025 · PwC, *EMEA Cloud Business Survey* — Middle East findings, April 2026.

Saudi Arabia. Law of Payments and Payment Services (Royal Decree M/26, 2021); SAMA Payment Services Provider Regulations; SAMA Cyber Security Framework v1.0 (May 2017); SAMA Business Continuity Management Framework v1.0 (February 2017); Personal Data Protection Law and SDAIA Data Transfer Regulations (September 2024); NCA Cloud Cybersecurity Controls CCC-2:2024; SAMA E-commerce Payments Interface (July 2025); SAMA open banking licensing framework (March 2026).

Qatar. QCB Payment Services Regulations (Circular 23 of 2021); QCB Data Handling and Protection Regulation (February 2025); QCB Cloud Computing Regulation (April 2024).

UAE. Retail Payment Services and Card Schemes Regulation (Circular C 15/2021); Consumer Protection Standards (Circular N 1158/2021); Outsourcing Regulation for Banks (Circular C 14/2021); Open Finance Regulation (Circular C 03/2025); Federal Decree-Law No. 6 of 2025; DFSA Prudential Investment Business Rules as amended 1 July 2026.

Egypt. CBE Rules for Licensing and Registration of Payment System Operators and Payment Service Providers (19 June 2025); Personal Data Protection Law 151 of 2020 and Executive Regulations (November 2025); FRA Decrees 139, 140 and 141 of 2023.

Other markets. Bahrain: CBB Rulebook Volume 5, Payment Service Requirements Module (February 2026) · Kuwait: CBK Resolution No. 45/471/2023 · Oman: National Payment Systems Law RD 8/2018; Banking Law RD 2/2025 · Jordan: Electronic Payment and Money Transfer Bylaw No. 111 of 2017 · Morocco: Law 103-12 on Credit Institutions and Similar Bodies.

Standards. PCI Security Standards Council: PCI DSS v4.0.1; FAQ 1588 (February 2025); guidance on Requirements 6.4.3 and 11.6.1.

Expert contribution. Gaurav Sachddeva, Co-Chair, MENA Fintech Association; Co-Founder and CEO of The Founders Majlis; former Head of Acceptance and Gateway Solutions at Mastercard MENA East. Akurateco DevOps and infrastructure team, September 2026.

Regulatory positions are stated as at September 2026 and provided for general information. They are not legal advice; licensing, capital and data residency requirements should be confirmed with local counsel before they are relied upon.

AKURATECO

Let's achieve your payment goals together.

Give us one hour to walk you through the full capabilities of our orchestration platform and how we can support your launch or expansion across the Gulf.

Book a demo →

wp@akurateco.com

+31 61 8330730

akurateco.com/on-premises-payment-gateway