MAHMOOD.INSIGHT

A SPECIAL EDITION · INTELLIGENCE, INFRASTRUCTURE AND DEPENDENCY

From Digital-First to Dependency-Aware

The Central Bank has declared the intelligence-first phase. Intelligence runs through providers — and no published instrument asks which providers the sector shares.

Special Edition
July 2026

Coverage
Sultanate of Oman

Audience
CBO · Boards · Risk

Mahmood Al-Hattali · Independent Strategic Advisor · Banking & Payments

mahmoodssh@gmail.com · +968 9507 2766

IN THIS PAPER

Contents

01 What digital-first built, and what it runs on 05

02 The rule and the exposure, same quarter 07

03 Why the instruments stop at the institution 08

04 Who can see the dependency picture 09

05 March 2026 — dependency failure demonstrated 11

06 Why intelligence-first raises the stakes 13

07 The international and regional reference layer 14

08 Becoming dependency-aware — four steps 18

A Evidence Register 20

B Verification Record 22

C Research Method 23

EXECUTIVE SUMMARY

The argument, in one page.

Institution-level supervision cannot, by itself, fully observe an exposure created by correlation across institutions. This paper is about the limits of institutional visibility, not the existence of institutional failure.

1 **The CBO has named the next phase.** Speaking in May 2026, CBO leadership described Oman's banking sector as moving from digital adoption to an "intelligence-first" phase in which AI, open banking and cybersecurity define financial services — with digital transactions at roughly 89% of volumes and instant payments running about 1.1 million a day.[1]

2 **Digital-first was measured. Dependency is not.** Oman publishes transaction volumes and values to nine-year series. It publishes nothing on which providers those transactions run through, or how many institutions share them.

3 **Intelligence increasingly runs through providers as well as banks.** Fraud scoring, AML monitoring and model inference are commonly bought rather than built, and a significant part of the layer is likely to depend on external providers, infrastructure or model components even where the bank retains the decision.

4 **No Omani bank publicly discloses a fraud, AML or model provider.** A search of bank disclosures, vendor announcements and trade press returns no named deployment — a research finding, not an allegation.

5 **Oman named this risk in 2011 and gave it to an addressee who cannot perform it.** Circular BM 1080 requires banks to ensure no undue reliance on a few providers "by many banks" — a sector-level test assigned to institutions that cannot see the sector.

6 **The pattern is structural, not an oversight.** A supervisor licenses institutions, so every instrument inherits "the licensed institution shall." When exposure sits between licensees, the rule reaches for the nearest addressee it has.

7 **Dependency-awareness is assembly, not construction.** The Systemic Risk Survey, the cloud pre-approval filings, the D-SIB methodology and the sector-circular precedent already exist. None is currently pointed at the shared layer.

FROM THE DESK

I spent eighteen years building on rails I could not see.

Retail banking product in Oman — cards, acquiring, deposits, lending, remittances. Every one of those products ran on infrastructure the bank did not own, could not inspect, and could not have replaced. That was normal, and it still is. This paper is about what it means now that the sector is adding intelligence on top of it.

In May 2026 the Central Bank told the market that Oman is moving from digital-first to intelligence-first banking. That is the right call and the numbers behind it are real. The question this paper asks is narrower: what has to be true underneath that phase for it to be as resilient as the one before.

The objection, stated first

A supervisory reader's first instinct will be that Oman already regulates this. That instinct is correct. There is an outsourcing circular, a cloud computing policy, and a Cyber Security & Resilience Framework with a dedicated third-party supply chain domain — a stronger instrument set than several neighbours had at the same date.

Anyone running a product line in an Omani bank can answer every question those instruments ask. Which vendors support this product. What the contract says. What happens if they fail. Those are answerable, and they get answered.

What no product owner can answer — because the information does not exist anywhere they can reach — is whether the bank across the road depends on the same provider. The instruments ask each institution about its own vendors. None asks what the sector shares.

> **THE THROUGHLINE**
>
> *Digital-first was measured in transactions. Intelligence-first will be measured in dependencies. Oman currently counts one and not the other.*

Editions 01 and 02 traced a market that crossed into digital faster than its institutions were built for, then began layering AI on the same rails. White Paper 02 named foundation-model concentration as the risk no single bank can see. This paper joins the two: payments is where the dependency argument can be proved from published Omani data, and intelligence is where it will matter more and be harder to see.

Two notes on stance. This paper is written in the belief that the CBO has built more than it is given credit for, and the argument is not that something was missed — it is that the next step in a trajectory already underway happens to change the unit of analysis. And because the CBO operates OmanNet, the RTGS, the ACH and the MPCSS itself, nothing here should be read as suggesting the central bank is a point of failure. The argument concerns visibility at sector level, not the reliability of any operator.

01 · WHAT DIGITAL-FIRST BUILT

RO 274 billion moved through it last year. Nobody holds its map.

The digital-first phase worked. Volumes are published, growth is documented, and the infrastructure held. What was never published is what all of it runs on — and that is the question intelligence-first inherits.

CLEARED IN 2024

RO 274bn

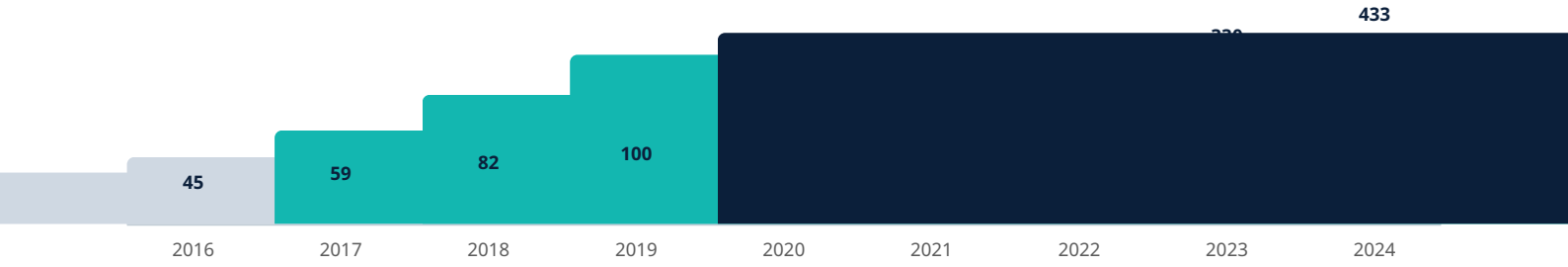
Total value through Oman's retail systems and RTGS combined — about RO 750 million every day.[1]

OMANNET, 2016→2024

9.6×

Transaction volume grew from 45m to 433m a year — roughly 1.2 million card transactions a day through one switch.[1]

OmanNet annual transaction volume, millions



Source: Financial Stability Report 2025, Payment System Indicators. The volume carried through the shared layer deepens each year.

01 · WHAT DIGITAL-FIRST BUILT, CONTINUED

Four kinds of commonality.

Diverse provider layer	**Core banking**	Finacle, Finastra, Temenos and iMAL — genuinely multi-vendor[2]
Shared infrastructure	**National switch · Clearing · Settlement**	OmanNet on one platform; ECC, ACH and MPCSS all settling into CBO-operated RTGS[3]
Common standard	**Open banking standard**	One mandated specification across all licensed participants — a common protocol, not a common provider[4]
Unmeasured provider layer	**Cloud, AI and vendor layer**	Extent of sharing across Omani banks is not publicly knowable[5]

Resilience does not aggregate upward. Four core banking vendors produce no redundancy if every core reaches the customer through the same switch and settles through the same rails.

And the usual remedy is unavailable here. A bank that reduced its dependency on the national switch would not become more resilient. It would become unreachable to every cardholder in the country.

> **THE DELIBERATE GAP IN THIS DIAGRAM**
>
> The top three layers are documented in primary sources. The fourth is not, and no research from outside the sector could close it. That is not a limitation of this paper — it is the finding, and Section 03 returns to who *can* see it.

1. Financial Stability Report 2025, Appendix 2, Payment System Indicators; RTGS value RO 240.5bn and total retail RO 33.8bn for 2024. Daily figures are the author's arithmetic on those totals. Tier P.

2. Finacle (Bank Muscat, Sohar International, Bank Dhofar), Finastra (NBO, Oman Arab Bank), iMAL/Path Solutions (Bank Nizwa). Vendors for Ahli Bank and Alizz Islamic are not publicly sourced. Tier S.

3. CBO operates four clearing systems settling into CBO-operated RTGS, relaunched 24/7 on 18 June 2023. OmanNet consolidated the former Al Shamel and Al Watani networks and links to GCCNet. Tier P / S.

4. Open Banking Regulatory Framework, §12.4 and §14.3.3. REST is the mandated default style; OAS 3.1.0 the specification. Architecture is decentralised — no central platform or directory operator is specified. Tier P.

5. No public source discloses cloud, fraud-engine or foundation-model dependencies at Omani bank level. The paper claims only that this is unmeasurable from outside. Tier Author.

02 · THE INSTRUMENTS

The rule and the exposure arrived in the same quarter.

The claim that Oman lacks third-party regulation is wrong, and worth killing early. The instruments exist, they are competent, and one of them names this exact risk. What they share is not a gap in coverage. It is an addressee.

Jan 2011
OmanNet goes live — Al Shamel and Al Watani consolidated into one national switch

Apr 2011
Circular BM 1080 warns against reliance on few providers "by many banks"

Sept 2023
CS&RF issued with a third-party supply chain domain

Feb 2025
Survey respondents rate shared-rail failure least severe

Mar 2026
One provider's facilities fail; banks in two states lose services

Read the first two markers together. In January 2011 the CBO consolidated Oman's card networks into a single national switch. In April 2011 — the same quarter — it issued a circular warning against concentration.

This is not an old rule that failed to anticipate modern infrastructure. It was written by people who could see what they were building.

CIRCULAR BM 1080, APRIL 2011 — THE CBO'S OWN COVERING TEXT

"...there is no undue reliance on one or a few service providers by many banks so as to engender concentration, systemic and other risks."[6]

STILL IN FORCE — AND NOW RE-CONFIRMED

Royal Decree 2/2025 replaced Oman's Banking Law on 1 January 2025. Its transitional provision states that existing regulations, decisions, instructions and circulars continue to operate to the extent they do not contradict the new law. BM 1080 does not contradict it, and appears in no subsequent circular as superseded. The instruction below is not a historical artefact. It is an operative supervisory instruction.[7]

The test is explicitly sector-level: reliance on a few providers *by many banks*. The circular lists concentration and systemic risk among the key risks in every outsourcing arrangement. The instruction is correct, current, and fifteen years old.

And no individual bank can discharge it. No Omani bank sees which providers its competitors depend on, or whether the system is converging on the same few. It can measure its own reliance. It cannot measure reliance "by many banks."

The obligation was sound. The addressee could not perform it.

6. Circular BM 1080, "Outsourcing," April 2011, para. 3(ii)(i); concentration and systemic risk also listed at para. 4. The circular attaches the 2005 Joint Forum principles, described in the covering text as a Basel Committee paper. Tier P. OmanNet go-live January 2011 per vendor announcement (Tier S); the two dates fall in the same quarter.

7. Royal Decree 2/2025 (Banking Law), transitional provision; CBO circular BM 1211 announcing its issue, January 2025. Existing circulars continue in force where not contradicted. Tier P / S. Verified against the CBO circulars index, July 2026.

03 · WHY THE INSTRUMENTS STOP AT THE INSTITUTION

Four instruments. One addressee. The pattern is not a coincidence.

INSTRUMENT	WHAT IT REQUIRES	ADDRESSED TO
BM 1080 — Outsourcing April 2011	Board-owned policy, due diligence, contractual rights, supervisory access, contingency planning	Each licensed bank
Cloud Computing Policy	Governing structures, risk assessment, data classification and residency	Each institution
CS&RF §3.4 September 2023	Risk assessment, due diligence, contract structuring, oversight; prior CBO approval for material cloud arrangements	Each institution
D-SIB Framework	Capital surcharge to 2.5%; substitutability an explicit designation criterion	Individual banks

Why every instrument lands in the same place

Four instruments, drafted over twelve years by different teams for different purposes, all arrive at the same addressee. That is not four independent choices. It is a structural property of how prudential regulation is written.

A banking supervisor licenses institutions. Its enforcement powers attach to licences, its reporting lines run to licensed entities, its sanctions bite on licensed balance sheets.

So every obligation begins "the licensed institution shall," however sector-minded the drafter. The unit of analysis is not chosen. It is inherited from the licensing perimeter.

> **THE LICENSING PERIMETER PROBLEM**
>
> A supervisor's strongest direct prudential powers ordinarily attach to the entities inside its regulatory perimeter. When the exposure sits with parties outside it — or in the correlation *between* licensees rather than within any one of them — the instrument reaches for the nearest addressee it has. This is why the same gap appears across jurisdictions with entirely different rulebooks. Closing it may require extending the perimeter for the most critical providers, but the visibility gap can begin to be addressed before that, through sector-level aggregation and testing.

This is what the UAE did in 2025, extending its licensing perimeter to technology providers enabling licensed financial activities. It is what the BCBS did in December 2025 by writing three of its twelve principles for supervisors rather than banks. Both are recognitions of the same thing: an obligation is only as good as the party it can be given to.

The pattern in the strongest instrument

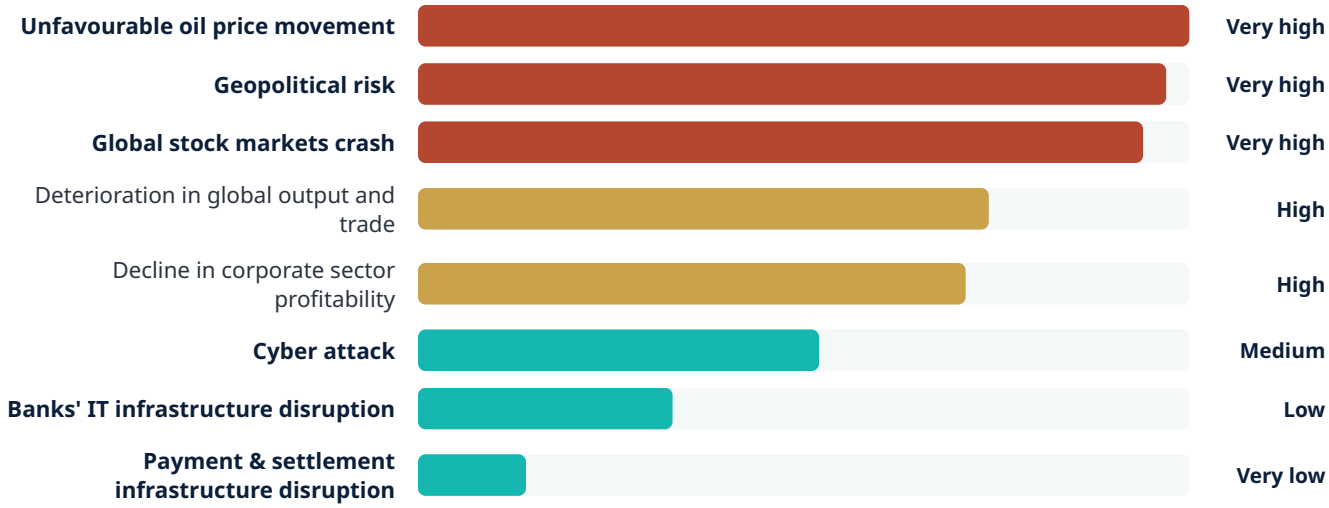
The CS&RF is a genuinely strong framework and predates comparable instruments in several neighbouring jurisdictions. Its third-party domain sets out four elements — risk assessment, due diligence, contract structuring, oversight.[8] Every obligation runs to the licensed institution and its own vendors. There is no aggregate or sector-level concentration provision anywhere in the domain. And the domain governs *cyber* supply chain risk specifically — while the most instructive recent regional disruption had a physical trigger.

8. Cyber Security & Resilience Framework, September 2023, §3.4 with §3.4.1 Contract and Vendor Management, §3.4.2 Cloud Computing, §3.4.3 Outsourcing. Tier P. The licensing perimeter argument is the author's analysis. Tier Author.

04 · THE ASYMMETRY

Invisible to the market. Visible to exactly one party.

Respondents placed shared-infrastructure failure among the six least severe of twenty risks. That judgement was not unreasonable — it was made without the only data that could have informed it, which sits with the supervisor.



Expected severity from the CBO's Systemic Risk Perception Matrix, Financial Stability Report 2025. Technology events in teal; intermediate rows omitted. Bar lengths indicate relative severity band, not survey scores.[9]

Why that answer was rational

It would be easy, and wrong, to read this as complacency. Ask what a respondent would need to answer well: how many institutions depend on the same provider, whether the sector is converging, what fails together. None of it is published. A respondent rating this risk in February 2025 was estimating something no available data could inform.

The asymmetry

Here is the feature that makes Oman a clearer case than most markets. Under CS&RF §3.4.2, every material cloud arrangement requires prior CBO approval, including scope of services and data classification. Those filings arrive institution by institution. And they arrive at one address.

WHO	CAN SEE	CANNOT SEE
An individual bank	Its own vendors, contracts and cloud arrangements	Whether peers share them
The market	Published aggregates and payment volumes	Any provider dependency
This paper	Three documented structural layers	The vendor layer beneath
The CBO	Every material cloud filing, from every licensed institution, already held	— nothing structural

04 · THE ASYMMETRY, CONTINUED

The technical failure ends first. The operational one does not.

FROM PRACTICE — HOW A DEPENDENCY FAILURE ACTUALLY PRESENTS

In day-to-day banking operations, dependency failures rarely present as a single clean outage. They appear first as operational uncertainty: front-line staff receive conflicting information, workarounds multiply, customer queues grow, reconciliation begins to lag, and responsibility fragments across teams. The technical failure is often resolved before the operational effects have fully unwound — and the second interval is the longer of the two.

This is why an institution-level continuity plan can be sound and still leave the sector exposed. Each plan assumes its own institution is the one recovering. None assumes every peer is recovering simultaneously, competing for the same vendor's attention. That distinction becomes more important, not less, as AI introduces additional shared decision-making components.[10]

THE ONE-LINE VERSION

The dependency picture is invisible to every participant in the Omani financial system except one — and that one already holds the filings needed to assemble it. What is missing is not authority, access or data. It is the aggregate view across records already collected.

The FSR goes further than the survey does. On cyber risk it notes that although Oman has not experienced a major event, *"the potential for cross border contagion or third-party provider compromise remains a material risk."*[11] The mechanism is named. What follows is description, not measurement.

9. CBO, Financial Stability Report 2025, Box 1.1 and Table 1.1.1. Survey responses collected February 2025; twenty events scored on probability and impact. Tier P.

10. Practitioner interpretation drawn from eighteen years in Omani retail banking product roles. Offered as informed judgement, not as a documented incident record. Tier Author.

11. FSR 2025, Section 2. Tier P. Visibility asymmetry is the author's analysis.

05 · THE CASE STUDY

One provider. Multiple banks. Two countries. No cyber attack.

In March 2026, cloud facilities in the UAE and Bahrain sustained physical damage. Financial services across two states were interrupted. The event has been reported through the lens of its cause. Read through the lens of its mechanism, it is the clearest concentration case study the Gulf has — and the recovery time is the part that matters most.

SERVICES REPORTING ERRORS

60+

More than 60 services were reported as experiencing errors or degraded availability across the two affected regions. This is a reported service count, not a count of independently confirmed infrastructure failures. [1][2]

RECOVERY TIME

Months

The provider stated recovery of the damaged UAE region would take several months — not hours or days.[1][2]

PROVIDER GUIDANCE

Migrate

Multinationals were advised to move sensitive workloads to decoupled external geographies. [1][2]

Why the framing matters

Almost every published account treats March 2026 through its cause. Not wrong, but it obscures the transmission mechanism — which is what matters for supervision. The banks affected did not share a location problem. They shared a provider.

Institutions with different core systems, different risk committees and different regulators failed the same way at once, because one layer beneath all of them was common.

Three features make it instructive for Oman specifically:

- **The trigger was physical, not cyber.** Cyber-specific third-party controls, including the CS&RF domain, would not by themselves have prevented a physical loss of regional infrastructure. Whether broader continuity and concentration controls anticipated the resulting correlated outage is a separate question.
- **It crossed jurisdictions.** Two national supervisors, each supervising its own banks competently, and neither positioned to see a dependency shared across both.
- **Each bank's own controls were arguably adequate.** There is no reported failure of institution-level due diligence. The exposure was correlation, which institution-level due diligence does not measure.

> THE POINT OF THE CASE
>
> *Correlated failure does not require an attacker sophisticated enough to breach many banks. It requires many banks to have made the same reasonable procurement decision.*

What Oman can and cannot conclude from it

The honest reading is bounded. There is no documented Omani or GCC shared-infrastructure outage prior to March 2026, and no public CBO response to it on the record. That absence should be read as exactly that — no public statement located — not as an inference about supervisory activity, which may well have occurred privately.

What the event does establish is that the scenario is no longer hypothetical in this region, and that it materialised through a vector no existing Omani instrument is scoped to catch — availability lost for reasons having nothing to do with an attacker. When the 2026 Systemic Risk Survey asks respondents to rate disruption of shared infrastructure, they will be answering a question the region has now seen tested.

05 · THE CASE STUDY, CONTINUED

The region diagnosed concentration. The remedy on offer is only half of one.

MONTHS, NOT HOURS

Continuity planning is generally written against outages measured in hours. A provider stating that regional recovery would take *several months* is a different category of event: long enough that fail-over is not a contingency but a migration, and long enough that every institution sharing that dependency attempts the same migration at the same time.

The region has now drawn a conclusion

One regional policy analysis argued the root problem was concentration — single-jurisdiction deployment offering no redundancy once the physical layer was compromised — and the proposed remedy is to make multi-cloud and multi-region redundancy a binding regulatory requirement rather than a best-practice recommendation.[13]

Right, and incomplete. A redundancy mandate tells each institution to spread its own exposure. It does not establish whether they have all spread it to the *same* second provider.

Redundancy without a dependency map produces correlated failover: the appearance of resilience, purchased separately by every bank, from the same narrow pool. Which returns the question to who holds the map.

13. ORF Middle East, June 2026, "Beyond Conflict: Fiscal and Digital GCC Resilience." Tier S.

12. Sequence separated by element. **Physical:** drone strikes, 1–2 March 2026 (Reuters, 2 March 2026). **Facility:** two UAE-region facilities struck directly, one Bahrain facility damaged by a nearby strike; structural damage, disrupted power, water damage from fire suppression (provider status statements). **Service:** 60+ services reported errors or degraded availability. **Recovery:** provider described recovery as prolonged and advised migration to alternate regions. Tier S throughout. Individual institutions are not named here: the argument concerns a shared provider, not the performance of any bank.

06 · WHY INTELLIGENCE-FIRST RAISES THE STAKES

Everything above is the payments case. The intelligence case may be harder on all three.

The shared-rail argument can be demonstrated from published Omani data. The intelligence-layer exposure cannot presently be demonstrated from an equivalent public series — and that difference is itself the argument.

AXIS	PAYMENTS LAYER	INTELLIGENCE LAYER
Substitutability	Low. A switch can in principle be re-platformed over years.	Lower. A model cannot be swapped without re-tuning thresholds and re-validating.
Distance from the perimeter	Inside it. The CBO operates the rails itself.	Outside it. A model sits behind a vendor, often behind a cloud.
Measurability	Unmeasured but measurable. Volumes published to nine-year series.	Unmeasured. No comparable public longitudinal series was located.

The third comparison is the finding

The first two are arguments. The third is a fact about the record. For payments, this paper built a chart from nine years of CBO-published volume. For the intelligence layer, no comparable publicly available longitudinal series was located — in Oman, the GCC, or internationally.

The thing a supervisor would want to measure does not currently produce a number.

> **A SOURCED NEGATIVE FINDING**
>
> A search of Omani bank disclosures, annual reports, vendor announcements and regional trade press returns *no publicly named fraud, AML or model provider at any Omani bank*. Banks do announce AI — for staff training, onboarding and fintech partnerships. The financial-crime and decisioning stack is not disclosed. Stated as what the public record contains, not as criticism: no disclosure obligation exists.[14]

What is visible

Two things are on the record and they point the same way. Oman Data Park has agreed to co-develop sector-specific AI for banking on sovereign cloud infrastructure, citing data residency and regulatory compliance, and operates five data centres expanding from 10MW toward 20MW explicitly to meet AI demand.[15] At least two banks have publicly disclosed relationships with that provider.[16]

Neither fact is a problem. A sovereign AI layer with local residency answers several risks at once, and matches the CBO's framing of cybersecurity as national security.

But it is the beginning of a shared dependency. And this paper's pattern applies: once more than a few institutions build on the same layer, the exposure stops being any one bank's to manage.

> **WHAT THIS PAPER DOES NOT CLAIM**
>
> That Omani AI dependency is currently concentrated. That cannot be established from public sources in either direction. What can be said is narrower and harder to dismiss: the intelligence-first phase has been declared, provider dependency is its operating premise, and no published instrument or dataset would reveal the concentration if it existed.

14. Search conducted July 2026 across bank disclosures, vendor press releases and regional trade press. Absence of public disclosure is not evidence of absence of deployment. Tier Author (research finding).

15. Oman Data Park announcements, April 2025 (sector-specific AI MoU covering BFSI on sovereign cloud) and October 2025 (OCI dedicated region, Ibri); capacity from CEO interview, September 2025. Tier S.

16. Bank Nizwa digital partnerships, June 2024; First Abu Dhabi Bank MoU, March 2025. Tier S. Disclosed relationships with a local infrastructure provider; neither is an AI-specific deployment on the public record.

07 · THE REFERENCE LAYER

The standard-setters moved. So did the neighbours.

Between December 2023 and June 2026, third-party concentration moved from specialist concern to settled supervisory agenda — and, in March 2026, from principle to operable rule. The mechanism this paper recommends is no longer hypothetical.

Body	Date	What it establishes
BCBS	10 Dec 2025	Principles for the sound management of third-party risk. Twelve principles — nine for banks, three for supervisors. Requires registers and mapping of all third-party arrangements and supply-chain parties. Supersedes the 2005 Joint Forum paper attached to BM 1080.[17]
IMF	5 Jan 2026	Good practices in cyber risk regulation and supervision. Five requirements including robust oversight of third-party service providers and sector-wide operational resilience strategies; recommends bringing critical technology service providers under direct oversight, and argues supervisory presence matters more than rule complexity.[18]
FSB	Dec 2023	Third-party risk toolkit — concentration risk, systemic dependencies, sector-wide exercises; explicitly proportionate for smaller institutions.[19]
FSB	Nov 2024 · Oct 2025	AI reports naming third-party dependency and service-provider concentration as systemic vulnerabilities.[19]
Bank of England	18 Mar 2026	Three aligned instruments issued the same day — BoE (financial market infrastructures), PRA PS7/26 and FCA PS26/2 (authorised firms). In-scope entities must notify material third-party arrangements and file an *annual register* of them. Effective 18 March 2027.[20]

07 · THE REFERENCE LAYER, CONTINUED

The register stopped being a proposal in March 2026.

The FSB's June 2026 Plenary listed operational outages at critical nodes among current vulnerabilities to financial stability — one item in a broader list, alongside asset valuations, sovereign debt and private credit.[21]

The Bank of England instrument matters for a different reason than the others. A register of material third-party arrangements, filed annually with the supervisor, is precisely the mechanism Section 08 of this paper proposes. It has now been drafted, consulted on, and given a compliance date by a major supervisor. The question of whether such a register is workable has been answered elsewhere.

And in July 2026 the same jurisdiction went one step further. The United Kingdom designated Amazon Web Services, Google Cloud, Microsoft and Oracle entities as its first critical third parties to the financial sector, with joint Bank of England, PRA and FCA oversight from 13 July. The regime subjects the systemic services those providers supply to regulated firms and financial-market infrastructures to direct resilience oversight — while expressly distinguishing designation from authorisation of the providers themselves. It is the clearest working example of the distinction this paper draws: a supervisor reaching a shared provider through resilience oversight, without treating that provider as a licensed financial institution.[20]

The BCBS paper remains the load-bearing citation, for a structural reason. Oman is Basel-aligned rather than bound by the EU's DORA regime, so a European critical-third-party framework is comparative material at best. The Basel principles are not. They sit within the reference frame the CBO already works to, address supervisors as well as banks, and supersede the very annex BM 1080 attaches.

07 · THE REFERENCE LAYER, CONTINUED

Where the GCC has moved.

Where the GCC has moved

- **UAE.** Federal Decree-Law 6/2025 consolidated banking, insurance and payments regulation and made the licensing perimeter explicitly technology-neutral: Article 62 reaches any person carrying on, offering, issuing or *facilitating* a licensed financial activity, whatever the medium or technology. The CBUAE has stated that this does not extend to technology service providers supplying software, infrastructure or solutions exclusively for the benefit of a licensed institution. Article 62 alone does not establish the full extent of the CBUAE's outsourcing, information-gathering or third-party oversight powers.[22]
- **UAE.** A dedicated Outsourcing Regulation with explicit aggregate and concentration language, a register, board approval and a no-objection requirement — the most specific instrument of its kind in the region.
- **Kuwait.** The Cyber and Operational Resilience Framework, December 2025, replaced the 2020 cyber framework with a resilience-first design extended to open banking service providers.
- **Saudi Arabia, Qatar, Bahrain.** Established cyber, outsourcing and cloud instruments at SAMA, QCB and CBB respectively.

07 · THE REFERENCE LAYER, CONTINUED

The perimeter follows the activity.

The UAE case is worth reading precisely. A supervisor rewriting its entire financial statute for a technology-mediated market extended its perimeter to whoever *performs* a financial activity, then drew an explicit line short of the firms that merely supply the performing institution. That is not an oversight; it is a coherent boundary. It is also the pattern this paper describes: the perimeter follows the activity, and the shared supplier sits outside it.

The sequence matters more than the ranking. Oman issued its Cyber Security & Resilience Framework in September 2023, ahead of several of these peers. What those peers are doing now is the step that follows a cyber framework: extending it from cyber to resilience, and from institutions to providers. Kuwait's December 2025 instrument replaced its own 2020 framework on exactly that logic. Oman is at the point in the cycle where this step comes next.

> **THE COMPARATIVE NOTE**
>
> Industry analysis published in January 2026 identified the central banks of the UAE, Kuwait, Jordan, Qatar and Bahrain as each working on new operational resilience regulations, some expected during 2026. Oman was not among those listed — on that survey, at that date.[23]

And the UAE case cuts both ways, which is the more useful reading. It has among the region's most developed third-party regimes — a technology-neutral licensing perimeter, a dedicated outsourcing regulation with explicit concentration language, a sovereign cloud programme. Its banks were still disrupted in March 2026. The lesson is not that rules fail. It is that instrument strength at institution level does not, by itself, resolve an exposure sitting at sector level.

17. BCBS, "Principles for the sound management of third-party risk in the banking sector," BIS d605, 10 December 2025. Tier P.

18. IMF Departmental Paper 2026/001, "Good Practices in Cyber Risk Regulation and Supervision," 5 January 2026. Tier P.

19. FSB third-party risk toolkit, December 2023; FSB AI reports, November 2024 and October 2025. Tier P.

20. Bank of England IOREP policy statement for FMIs; PRA PS7/26; FCA PS26/2 — all 18 March 2026, effective 18 March 2027. Only ***material*** third-party arrangements are registrable. Tier P.

21. FSB Plenary, London, 1 June 2026 (press release ref. 8/2026). The Plenary listed operational outages at critical nodes among current vulnerabilities; it is one item in a broader list, not a headline finding. Tier P.

22. UAE Federal Decree-Law 6/2025, Art. 62, in force 16 September 2025, read against the CBUAE's published position. Art. 62 reaches persons carrying on, offering, issuing or facilitating a licensed financial activity through any medium or technology. The CBUAE states it does not thereby regulate technology service providers supplying software, infrastructure or solutions exclusively for the benefit of a licensed institution. Tier P.

23. KPMG, January 2026. Secondary compilation used to identify potential regulatory examples; load-bearing examples independently verified against primary materials. Items not independently verified are not presented here as settled regulatory facts. Contextual, non-evidential.

08 · BECOMING DEPENDENCY-AWARE

Start with a form change. Everything else sequences behind it.

Offered for consideration, not prescription — the rulebook is the CBO's to write. What follows is ordered by cost. The first step is a question added to a survey that already goes out.

01 · Measure	02 · Map	03 · Test	04 · Designate
Next FSR cycle	From data already held	Existing circular power	Once 01–03 show where

The order matters. Designation without a map is guesswork; a map without a measurement has no baseline.

1 Add one category to the Systemic Risk Survey

Insert a twenty-first event: *failure of a third-party provider shared across multiple institutions* — distinct from "banks' IT infrastructure disruption," which respondents read as their own estate. One line on a form that already circulates each February.

Already exists: the instrument, the respondent panel, the publication vehicle.
What changes: one question.

COST: NEAR ZERO

Deliverable in the next survey cycle. Creates the first published baseline of how sector participants perceive shared-provider failure.

2 Aggregate the cloud approvals already on file

CS&RF §3.4.2 requires prior CBO approval for every material cloud arrangement, including scope and data classification. Those filings, read across institutions rather than one at a time, could provide the first cloud-dependency map across regulated institutions — then be extended toward a broader third-party register. Publish the concentration picture — not institution-level detail — in the FSR. The format is no longer novel: the UK has adopted aligned annual-register requirements for material third-party arrangements across supervised financial market infrastructures, PRA-authorised firms and FCA firms. Oman's advantage is that the underlying filings already arrive.

Already exists: the filings, the legal basis for holding them, the reporting channel.
What changes: the axis they are read along.

COST: ANALYTICAL ONLY

Likely no new first-layer data collection; implementation remains subject to confirmation of confidentiality, data-use and publication powers. The inputs are in the building — and a workable template now exists abroad.

3 Run one sector-wide exercise against shared-rail failure

Move beyond bank-by-bank continuity attestation to one coordinated exercise assuming a shared dependency is unavailable. Domestic precedent exists: in March 2020 the CBO issued sector-wide circulars directing banks, exchange and finance companies to assess risks and ensure continuity of core operations.[24]

Already exists: the circular power and a precedent for using it at sector scale.
What changes: testing the shared layer rather than each institution's own.

COST: COORDINATION

One exercise, scoped to a single scenario, is worth more than a broad programme deferred.

08 · BECOMING DEPENDENCY-AWARE, CONTINUED

The last step is the only one that needs new instrument text.

4 **Designate critical providers — once the map says which**

Establish a critical service provider concept using the four criteria already in the D-SIB methodology: systemic impact, systemic importance of dependents, reliance for critical functions, and substitutability. Pair it with a dedicated outsourcing regulation. Extend monitoring — not yet designation — to AI and fraud-model providers.

Already exists: the designation machinery and the substitutability criterion. **What changes:** the class of entity it reaches.

COST: RULEMAKING

The only step needing new instrument text — and the one steps 01–03 make evidence-based rather than speculative.

ON MACHINERY

Steps 1–3 appear capable of beginning within existing supervisory channels, subject to confirmation of confidentiality, data-use and publication powers; Step 4 would require formal instrument design. The Joint Financial Stability Committee already exists. Oman designates at institution level (D-SIB) and at national-infrastructure level (CNI). The missing tier is the financial-sector shared provider, between the two.

24. Oman News Agency, March 2020 (Arabic) — CBO sector-wide circulars on cyber vigilance, risk assessment and continuity of core operations. Tier P.

APPENDIX A · EVIDENCE REGISTER

Every claim, its source, its tier.

P = primary institutional or official publication, read directly. S = secondary or industry reporting. Author = the paper's own inference, labelled as such.

Claim	Source	Tier
Payment volumes and values; nine-year series	FSR 2025, Appendix 2	P
Systemic Risk Survey — twenty events, six rated "Very Low"	FSR 2025, Box 1.1, Table 1.1.1	P
Third-party provider compromise described as a material risk	FSR 2025, Section 2	P
BM 1080 sector-level reliance test	Circular BM 1080, April 2011, para. 3(ii)(i)	P
BM 1080 operative under the Banking Law transitional provision	Royal Decree 2/2025; CBO circulars index	P
CS&RF third-party domain; cloud pre-approval	CS&RF, September 2023, §3.4	P
Open banking architecture is decentralised	Open Banking Regulatory Framework, §12.4, §14.3.3	P
Four CBO clearing systems settling into CBO-operated RTGS	CBO; IMF 2025 Transparency Code Review	P
D-SIB framework; substitutability as designation criterion	CBO D-SIB Framework	P
March 2020 sector-wide cyber circulars	Oman News Agency, March 2020	P
UK annual register of material third-party arrangements	BoE IOREP; PRA PS7/26; FCA PS26/2 — 18 Mar 2026	P
Operational outages at critical nodes listed among vulnerabilities	FSB Plenary, 1 June 2026, ref. 8/2026	P
UAE perimeter reaches conduct of licensed activity; vendor carve-out	DFL 6/2025 Art. 62; CBUAE published position	P
BCBS third-party principles; IMF cyber supervision paper	BCBS December 2025; IMF 2026/001	P

APPENDIX A · EVIDENCE REGISTER, CONTINUED

Secondary and author-tier claims.

Claim	Source	Tier
UK designated first four critical third parties; resilience oversight, not authorisation	Critical Third Parties (Designation) Regulations 2026; BoE/PRA/FCA, 13 July 2026	P
Core banking vendor mix across Omani banks	Vendor and institutional announcements	S
OmanNet platform and consolidation date	Vendor announcement	S
March 2026 physical damage, service errors, recovery guidance	Reuters 2 Mar 2026; provider statements; regional reporting	S
CBO "intelligence-first" framing; ODP sector AI; two disclosed bank relationships	Press reports May 2026; ODP announcements 2025	S
Licensing perimeter as the structural cause of the shared addressee	Author analysis	Author
Potential correlated implementation exposure under a mandated common standard	Author analysis	Author
Three-axis comparison of payments and intelligence layers	Author analysis	Author
Operational tail of a shared-dependency failure	Practitioner interpretation	Author

APPENDIX B · VERIFICATION RECORD

What was checked, how, and what remains open.

Sources verified against primary materials in July 2026. Propositions that failed verification were removed rather than softened; one is recorded below.

Source	Method	Basis	Result
BM 1080 status under Royal Decree 2/2025	Transitional provision read; CBO circulars index checked	Primary	Confirmed in force
UAE DFL 6/2025, Article 62	Statute and CBUAE published position read directly	Primary	**Rejected as vendor-perimeter evidence** — reframed
FSB Plenary, June 2026	Primary release located and read (ref. 8/2026)	Primary	Confirmed; narrowed to one listed vulnerability
UK third-party reporting regime	Three instruments separated by supervised population	Primary	Confirmed; earlier description had understated scope
March 2026 disruption	Causal chain verified element by element across independent reports	Secondary	Confirmed; earlier service-failure count removed as unsupported
KPMG regulator compilation	Not decomposed to primary sources	Secondary	Retained as contextual only; non-evidential
Omani AI, fraud or AML provider disclosure	Search of bank disclosures, vendor announcements, trade press	—	Negative finding: none located

Outstanding at publication

Provider and wire originals for March 2026 beyond those cited; the KPMG list against each authority's own publications; the licensed bank count against the CBO Annual Report. None is load-bearing for the central claim.

APPENDIX C · RESEARCH METHOD

How the paper was built.

Scope

Publicly available material only. Primary Omani sources — the Financial Stability Report 2025, Circular BM 1080, the Cyber Security & Resilience Framework and the Open Banking Regulatory Framework — were read in full rather than through secondary description. No confidential, internal or client information informed any part of this paper.

Negative findings

Where a search returned nothing, that is reported as a negative finding rather than omitted. The principal one: no Omani bank publicly discloses its cloud, fraud-engine, AML or model provider. The absence is the finding, and it is what makes the exposure unmeasurable from outside.

Inclusion criteria

Regulatory instruments are cited where the text was read directly. Secondary reporting is used for events and market structure, and labelled S. Author-tier statements are inferences from the material and are marked as such, so a reader can separate what is documented from what is argued.

Terminology

Four kinds of commonality are distinguished throughout and not treated as equivalent: a *diverse provider layer* (many vendors, genuine choice); *shared infrastructure* (one operator, no substitute); a *common standard* (one specification, many implementers); and an *unmeasured provider layer* (extent of sharing not publicly knowable).

Limitations

This paper cannot establish the degree of provider concentration in Oman, because the information required is not public. It argues that the question is currently unanswerable from outside, and that the answer would be assembled from filings the supervisor already holds. It is about the limits of institutional visibility, not the existence of institutional failure.

This paper synthesises publicly available information for analytical and discussion purposes. It is not investment, legal, or regulatory advice, and represents no institution's position. Figures are accurate to the author's knowledge at time of publication; readers should consult primary sources for definitive data. © Mahmood Al-Hattali, 2026.

CLOSING

Digital-first was measured. Intelligence-first has to be too.

Oman counted the digital-first era carefully. Nine years of volumes and values, published annually, is why this paper could chart it. The intelligence-first era has been declared with the same seriousness — and currently has no equivalent measure of what it runs on.

Apply the same criterion to the shared layer and a different question appears. National payment rails are structurally difficult to substitute, while common cloud or technology providers could create correlated disruption wherever several institutions depend on the same service. The public record does not show the full extent of that dependence, and therefore cannot establish which providers, if any, warrant sector-level designation. That is precisely the visibility gap this paper asks the supervisor to measure.

That is not an oversight so much as an artefact of when the frameworks were written. Every instrument Oman has was built when the sensible unit of analysis was the institution. The instruments are sound. The world beneath them changed shape, and in March 2026 the region saw what that shape does under stress.

The question that makes a sector dependency-aware

Which providers could the Omani banking system not function without?

No individual bank can answer it. The supervisor can — and the first step is a single category added to a survey that already goes out each February.

This is a special edition of *The State of Omani Banking & Payments*, published outside the quarterly series because the March 2026 case study is time-sensitive and the next scheduled edition is the year-one prediction scorecard.

Next edition: Q1 2027 — the annual scorecard, grading Editions 01 and 02 predictions on the published scale.

Mahmood Al-Hattali
Independent Strategic Advisor · Banking & Payments · Muscat
mahmoodssh@gmail.com
+968 9507 2766

Correspondence on the findings in this paper — including corrections — is welcome.