NEXAPAIR WHITE PAPER · NOVEMBER 2026

Article 13, made practical

A field guide to third-party risk management under the Central Bank of the UAE's Operational Risk Management Regulation, C 1/2026

Published by NexaPair, a Kayak Strategic Advisors product · www.nexapair.com
This paper is for general guidance and is not legal advice. Always refer to the official text in the CBUAE Rulebook.

1. Executive summary

The Central Bank of the UAE's Operational Risk Management Regulation, C 1/2026, has been in force since 14 September 2026. It makes the management of third parties part of each institution's own operational resilience, and it keeps the Board accountable for work that is outsourced.

For most institutions the regulation does not invent a new discipline. It raises the standard of evidence. Questionnaires, annual reviews and contract folders are no longer enough on their own; the Central Bank expects a live register, risk-based due diligence before engagement, contracts that guarantee access and audit, continuous monitoring, tested exit plans and fast incident reporting.

Five things to do first

1. Get a Board-approved third-party risk strategy and policy in place (Article 13.1).
2. Build one register of outsourced activities and keep it current (Article 13.9.1).
3. Map which third parties support your Critical Operations (Articles 3.4 and 13.10).
4. Check every material contract for audit, access, termination and subcontracting terms (Articles 13.6 to 13.8).
5. Rehearse the 4-hour incident notification with your critical vendors (Article 15).

Done well, this work pays back: fewer disruptions, less fraud and leakage, faster onboarding, better negotiating positions and fewer costly remediation projects. Section 6 explains how.

Who this paper is for

Chief Risk Officers, heads of procurement, compliance, information security, operations and internal audit at institutions licensed by the Central Bank of the UAE, and the Board members who oversee them.

2. Why regulators focused on third parties

Financial institutions now depend on a long chain of providers: cloud platforms, payment processors, core banking and software vendors, call centres, sales agents and data providers. Customers experience the work of these providers as the bank's own. When one of them fails, the bank fails its customers.

Recent years showed how far a single weak link can reach. A compromised software update in 2020, a breached file-transfer tool in 2023 and a faulty security update in July 2024 each spread to thousands of organisations at once. Concentration adds to the risk: many institutions rely on the same small group of technology providers.

Financial crime follows the same routes. Fake vendors, conflicts of interest between staff and suppliers, and intermediaries that move money for sanctioned parties are all third-party risks.

Supervisors have responded worldwide. The Basel Committee published principles for operational resilience in 2021, and the European Union's Digital Operational Resilience Act has applied since January 2025. Regulation C 1/2026 brings the UAE in line with this direction.

3. What the regulation asks, article by article

The table summarises the main third-party requirements and the evidence that typically satisfies them. Article numbers follow the regulation; wording is paraphrased.

Article	What it requires	Evidence that works	Usual owner
4.1, 4.2	The Board is ultimately responsible for operational risk, including outsourced activities, and oversees it.	Board minutes approving the policy; regular Board reporting on third-party risk.	Board, CRO
3.4	Map Critical Operations, including the third parties that support them.	A current map linking each Critical Operation to its people, systems and providers.	Operations, Risk
8.9	Keep the master system of record in the UAE, including where activities are outsourced.	Data-location records per system and provider; contract clauses on data location.	IT, Legal
13.1	A Board-approved third-party risk strategy and policy.	Approved policy, risk appetite, tiering method and approval chains.	Risk, Board
13.2	Avoid over-reliance on outsourcing.	Concentration and single-source analysis; dependency reporting.	Risk, Procurement
13.3	Assess risk and carry out due diligence before engaging.	Tiering result; due diligence file proportionate to the tier, completed before signature.	Procurement, Compliance
13.4	Providers of Critical Operations must offer equivalent operational resilience.	Recovery objectives compared with your disruption tolerances; test results.	Operations, IT
13.5	Obtain the Central Bank's non-objection before outsourcing that affects Critical Operations.	Non-objection on file before go-live; a gate in your onboarding workflow.	Compliance

13.6	Written contracts covering rights and obligations, data ownership, confidentiality, termination, and inspection and audit rights for critical arrangements.	Clause checklist per contract; exceptions approved and recorded.	Legal
13.7	Central Bank access to the provider, including on-site examination.	Access clause in every relevant contract.	Legal
13.8	Subcontractors are bound by the same access and contract terms.	Flow-down clauses; a register of material subcontractors.	Legal, Procurement
13.9.1	Maintain a register of outsourced activities.	One complete, current register (see our template).	Procurement, Risk
13.9.2, 13.9.3	Monitor performance with metrics and assess providers on an ongoing basis, including financial condition.	Service-level data, review records, financial-health monitoring, screening alerts.	Business owners, Risk
13.9.4	Manage dependencies.	Dependency and relationship analysis, including links to your own staff.	Risk
13.10	Business continuity planning that covers Critical Operations and their providers.	BCPs referencing providers; joint tests.	Operations
13.11	Contingency and exit plans, considering how substitutable the provider is.	Exit plan per material arrangement, with alternatives and a test date.	Business owner, Procurement
13.12	The Central Bank may require an arrangement to be discontinued.	An executable exit plan and off-boarding procedure.	Business owner
15.2, 15.3	Notify the Central Bank of operational risk events affecting Critical Operations within 4 hours, provide a summary within 24 hours, notify the return to normal, and report high-risk incidents within 72 hours.	Incident playbook with providers; notification templates; time-stamped records.	Operations, Compliance

4. Who does what: the department dial

Third-party risk fails when it belongs to one team. It works when every department does a small, clear part. The table shows a practical split.

Department	Its part	Typical tasks
Procurement	Bring vendors in cleanly	Register the vendor, choose the service, send the supplier questionnaire, keep the register current.
Finance	Pay the right party	Confirm the bank-account owner before the first payment; hold payments when details do not match.
Legal	Contracts that hold up	Check audit, Central Bank access, data, termination and subcontracting clauses before signature.
Compliance	Screen and decide	Sanctions, PEP, adverse media and litigation checks; record each decision with its evidence.
Information Security	Safe access	Assess data and system access; set access levels; review security findings.
Operations	Resilience	Map Critical Operations; compare recovery times with tolerances; own exit plans.
HR	Conflicts of interest	Keep the employee list current so links between staff and vendors can be found.
Risk	The model	Set tiers, weights and thresholds; report to the Board; approve exceptions.
Internal Audit	Assurance	Sample decisions and test the evidence trail.
Board	Oversight	Approve the policy and related-party arrangements; review the Board pack.

5. A 90-day readiness plan

Days 1 to 30: see

- Collect every contract and supplier list into one register.
- Agree the tiering method and the Critical Operations list.
- Draft the policy for Board approval.
- Load the employee list for conflict checks.

Days 31 to 60: check

- Tier every third party; verify critical and high-tier vendors at the source.
- Review contracts for the required clauses; plan remediation.
- Map providers to Critical Operations and compare recovery times.
- Agree incident notification steps with critical vendors.

Days 61 to 90: prove

- Switch on continuous monitoring.
- Write and test exit plans for the most critical providers.
- Run a 4-hour notification drill.
- Present the first Board pack.

6. From cost to value

Many institutions see third-party risk management as a compliance cost. Done well, it pays its way:

- **Fewer disruptions.** Weak or over-stretched suppliers are found before they fail you.
- **Less fraud and leakage.** Fake vendors, wrong bank-account owners, duplicate vendors and staff conflicts are caught before money leaves.
- **Faster onboarding.** Data verified at the source replaces weeks of chasing documents.
- **Better buying.** One register shows exactly whom you depend on and what you pay, which supports consolidation and negotiation.
- **Fewer penalties and remediation projects.** Evidence is ready before the regulator asks.
- **Better use of experts.** Routine checks are automated; specialists spend their time on judgement.

7. Readiness self-check

Answer yes or no. Each “no” is a priority for the next quarter.

#	Question	Article
1	Has the Board approved a third-party risk strategy and policy in the last twelve months?	13.1
2	Do you have one register of outsourced activities that is complete today?	13.9.1
3	Can you name the third parties behind each Critical Operation?	3.4, 13.10
4	Is due diligence always completed before signature, at a depth set by risk tier?	13.3
5	Do critical providers’ recovery times sit within your disruption tolerances?	13.4
6	Is Central Bank non-objection on file for every arrangement that needs it?	13.5
7	Do all material contracts include audit, Central Bank access, data, termination and subcontracting terms?	13.6 to 13.8
8	Are vendors re-screened automatically, including financial condition?	13.9.3
9	Is there a tested exit plan for every critical provider?	13.11
10	Could you notify the Central Bank within four hours of a third-party incident today?	15

8. Glossary

Critical Operations: operations whose disruption would cause significant harm to customers, the institution or the financial system. **Material outsourcing:** an arrangement whose failure would significantly affect the institution. **Disruption tolerance:** the maximum disruption an institution accepts for a Critical Operation. **Substitutability:** how easily a provider could be replaced. **Master system of record:** the authoritative source of an institution’s records. **Non-objection:** the Central Bank’s confirmation that it does not object to a proposed arrangement.

Important. This paper summarises and paraphrases the CBUAE Operational Risk Management Regulation for general guidance. It is not legal advice and may not reflect later amendments, standards or guidance. Refer to the official text at rulebook.centralbank.ae and take professional advice for your institution. NexaPair helps institutions meet these requirements; responsibility for compliance stays with each institution.

© 2026 Kayak Strategic Advisors. You may share this paper in full with attribution.