citadel

VERTEX COMPLIANCE

CBUAE's Operational Risk Regulation:

A Guide for Financial Institution



Inside the CBUAE's 2026 Operational Risk Management Regulation

www.citadel365.com info@citadel365.com

About Speakers



Vasantha Mohan

Vasantha holds a Master's in Law specialising in Banking Laws and Anti-Money Laundering and is CAMS and CGSS certified. With over 35 years of experience, she has worked closely with regulators and international financial institutions, building financial crime risk frameworks, sanctions monitoring programmes, and compliance systems across multiple jurisdictions.



Sridhar Rajam

Sridhar is a Certified Anti-Money Laundering Investigator (CAMI) with over 30 years of experience in compliance, risk, and audit, including more than 20 years in AML and financial crime prevention. He has contributed to the development of UAE regulatory standards through the FERG sub-committee and has maintained active engagement with the Central Bank of the UAE on supervisory and compliance matters.

citadel

VERTEX COMPLIANCE

About Us

01

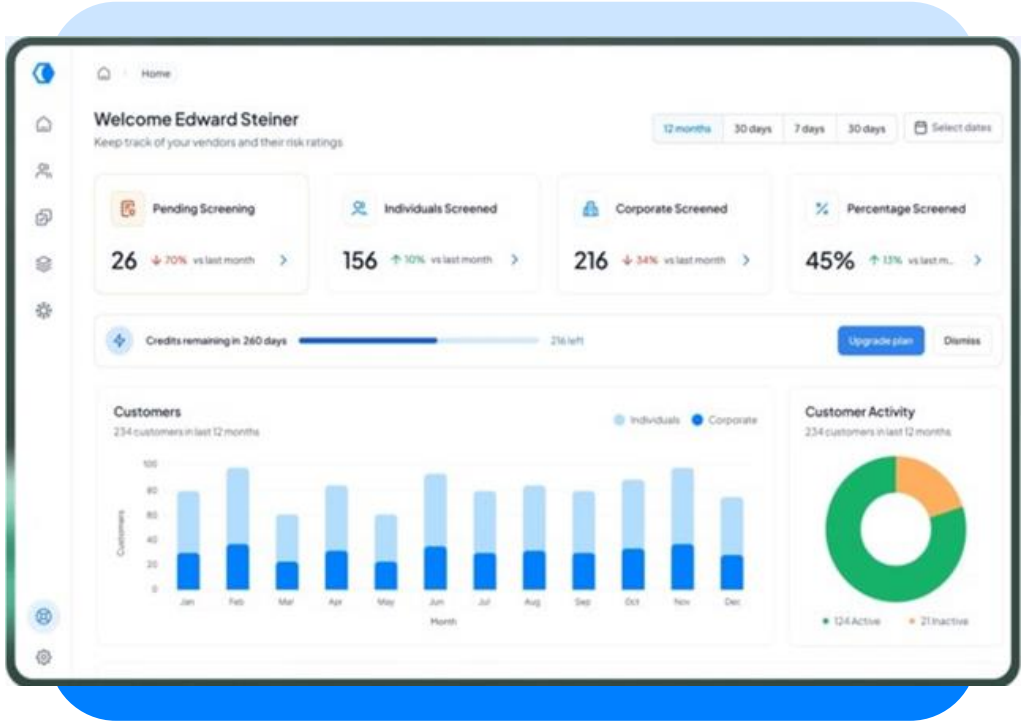
About Citadel365

Citadel365 is a single, integrated AML/CFT platform that turns episodic checklists into a continuous, auditable compliance lifecycle, built by AML/CFT veterans from Vertex Compliance.

Citadel365 supports:

- Customer onboarding with self-KYC and document capture, which shortens the onboarding life cycles
- Sanctions, PEP, and adverse media screening in real time with exportable, timestamped records
- Risk assessment module with configurable scoring, thresholds, and weightages
- Case management with clear controls and audit trails

The software supports DNFBPs, VASPs, banks, fintechs, financial institutions, and regulated entities, shaping their compliance practices for what comes next.



citadel

VERTEX COMPLIANCE

About Vertex Compliance

Vertex Compliance is a leading provider of comprehensive compliance and risk management solutions, dedicated to helping businesses navigate complex regulatory environments.

Vertex specialises in AML, KYC, and regulatory compliance, offering tailored solutions to meet the unique needs of various industries.

We also provide consulting services pertaining to FATCA/CRS, Data Protection Laws, and Trade Finance Compliance.



Disclaimer

- ✓ This session is intended to enhance compliance awareness and operational readiness.
- ✓ It does not constitute legal advice.
- ✓ Requirements may vary by sector, supervisory authority, and licence conditions.
- ✓ Entities should align final implementation with applicable UAE laws, executive regulations, and sector-specific guidance.

citadel

VERTEX COMPLIANCE

An Overview of This Session

01

The regulation at a glance

Scope, definitions and the framework requirements in Articles 1 through 3.

02

The governance backbone

Board and Senior Management accountability under Articles 4 through 7.

03

The operational core

ICT, incidents, data and business continuity under Articles 8 through 11.

04

Extending the compliance perimeter

Change management, third parties, Shari'ah risk, disclosure and enforcement under Articles 12 through 17.

05

Where to start

A practical sequencing for the months between now and the effective date.

citadel

VERTEX COMPLIANCE

The Regulation at a Glance

Scope, definitions and the framework requirements upon which the remaining provisions are constructed.

02

ART. 1 ART. 2 ART. 3

citadel

VERTEX COMPLIANCE

A New Minimum Regulatory Standard for the Sector

Introduced by Circular No. 1/2026, dated 3 February 2026.

Issued under the powers vested in the Central Bank by Federal Decree-Law No. (6) of 2025.

Sets the minimum regulatory requirements for Operational Risk and Operational Resilience across all Licensed Financial Institutions.

Cancels and replaces Circular No. 163/2018, the previous Operational Risk Regulation and Standards, in full.

Comes into effect one calendar month after publication in the Official Gazette.

Comprehensive Scope, Narrowly Defined Exclusions



Banks

Any juridical person licensed primarily to take deposits, plus other financial activities.



(Re)Insurance Companies

Insurance and reinsurance companies licensed under the Central Bank Law.



Other Financial Institutions

Any other licensed entity carrying on a Licensed Financial Activity.



Islamic Finance Institutions

The above, where they operate under Shari'ah principles, plus Article 14 obligations.

From a Risk Register to an Operating Model for Resilience

2018 REGULATION

- Operational Risk management only
- Governance duties described at a high level
- No explicit, standalone resilience framework
- Third-party oversight addressed lightly
- No formal change-notification regime

2026 REGULATION

- Operational Risk and Operational Resilience, fully integrated[1]
- Board's ultimate responsibility made explicit and non-delegable[2]
- Mandatory Critical Operations mapping [3]
- Third-party risk formalised, with CBUAE non-objection triggers [4]
- New change-management gate: expert review, 30-day notice, written non-objection[5]

1. (Article 2 & 3) 2. (Article 4.1) 3. (Article 3.4) 4. (Article 13.5) 5. (Article 12.5)

A Unified Approach to Risk and Resillience

ARTICLE 2

Operational Risk Management

- ✓ Identify
- ✓ Assess and evaluate
- ✓ Monitor and report
- ✓ Control or mitigate, on a timely basis

+

ARTICLE 3

Operational Resilience

- ✓ Respond
- ✓ Adapt
- ✓ Recover
- ✓ Learn, and reincorporate into the framework

The Regulation requires these two disciplines to be fully integrated rather than administered as parallel programmes. In practice, this requires a Disruption Tolerance Statement to accompany the Risk Appetite Statement, both reviewed by the same governance forum.

Four Terms That Shape the Regulation's Application

ARTICLE 1

Critical Operations	Functions, activities and their supporting assets whose disruption would materially affect financial stability, the institution itself, or its customers.[1]
Critical Information Assets	Data assets whose confidentiality, integrity or availability underpins those Critical Operations, or the institution's legal and regulatory compliance.[2]
Risk Appetite vs Risk Tolerance	Appetite denotes the level of risk an institution is willing to assume [3]. Tolerance denotes the permissible variance around that appetite.[4]
Third-Party Service Provider	Broader than outsourcing: any person performing services, activities or tasks directly for the institution, excluding its own employees.[5]

1. Article (1.10) 2. Article (1.09) 3. Article (1.25) 4. Article (1.27) 5. Article (1.31)

citadel

VERTEX COMPLIANCE

The Minimum Requirements of the ORM Framework

ARTICLE 2

- ✓ A governance structure with clear reporting lines, responsibilities and delegated authority
- ✓ A documented Risk Appetite and Tolerance statement for Operational Risk
- ✓ Tools to identify and assess risks and controls, used consistently by all three lines of defence
- ✓ Common terminology and standards across the institution, and the group where relevant
- ✓ Calibrated risk limits and thresholds, including a clear definition of a material operational loss
- ✓ Ongoing monitoring, regular reporting, and approved mitigation strategies and instruments

citadel

VERTEX COMPLIANCE

Mapping Critical Operations

ARTICLE 3

Every downstream obligation, continuity planning, incident management, third-party oversight, refers back to this single map. Establishing it with rigour at the outset yields recurring value across the framework.

People — **Technology** — **Processes** — **Data** — **Facilities** — **Third parties**

together with the interdependencies among them, rather than each asset considered in isolation

At minimum, the following must be treated as critical:

- Payment systems and other time-critical services for customers
- The ability to keep accurate, up-to-date financial records
- Timely measurement and management of solvency and liquidity
- Anything the Central Bank separately designates as critical

citadel

VERTEX COMPLIANCE

The Governance Backbone

The allocation of accountability, from the Board through the three lines of defence.

03

ART. 4 | ART. 5 | ART. 6 | ART. 7

Board Accountability: Absolute and Non-Delegable

ARTICLE 4

- Ultimate responsibility for the ORM framework sits with the Board itself, regardless of any committee set up beneath it.
- Must personally approve and review, at least annually: the Risk Appetite and Tolerance statement, the tolerance for disruption, and the BCP and Disaster Recovery Plans.
- Business Continuity and Disaster Recovery Plan review can be delegated to a committee, but the Board approves the initial plans and revisits them itself at least every three years.
- Must approve, oversee and ensure the effectiveness of the ICT and cybersecurity risk framework directly.
- Systemically important LFIs need a dedicated Board Operational Risk committee, or another designated committee with that mandate.

Senior Management’s Mandate: Operationalising Board Strategy

ARTICLE 5

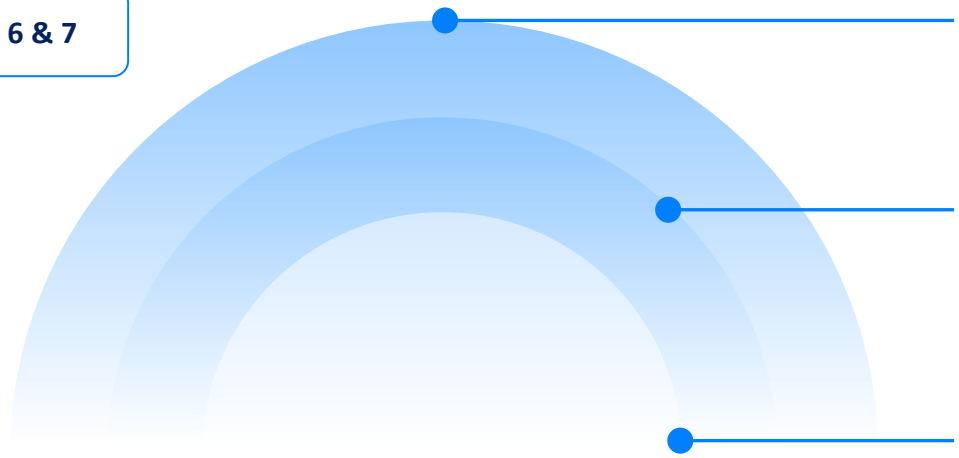
- Turns the Board-approved framework and resilience strategy into effective, well-implemented policies, processes and systems across the institution.
- Any breach, or expected breach, of Risk Appetite or Tolerance goes to the Board itself, in a timely manner, never routed only through a committee.
- Owns resourcing: sufficient staff, expertise and authority for internal control, change management and risk management, proportionate to each business line.
- Monitors the Operational Risk profile and material exposures on an ongoing basis, and reports to the Board regularly, not only when asked.
- Produces an annual Report on Internal Control (at minimum for Banks and (Re)Insurers), covering the key controls for all processes tied to Critical Operations.

citadel

VERTEX COMPLIANCE

Three Lines of Defence, Underpinned by a Formal Control System

ARTICLE 6 & 7



Line 1

Business Units

Identify and control Operational Risk on an ongoing, day-to-day basis.

Line 2

Risk & Compliance

The Operational Risk function, under the CRO, plus Compliance. Challenge, standard-set, and maintain the risk register.

Line 3

Internal Audit

Independent assurance over the whole framework, reported directly to the Board.

The internal control system underneath must address four components:

- **Risk assessment**
- **Control activities**
- **Monitoring activities**
- **Information & communication**

Article 7.4 specifies concrete control measures, among them segregation of duties, dual control, systematic limit monitoring, and a minimum-leave policy for staff in sensitive roles.

citadel

VERTEX COMPLIANCE

The Operational Core

ICT and cybersecurity, incident management, data integrity, and continuity planning.

04

ART. 8 | ART. 9 | ART. 10 | ART. 11

ICT and Cybersecurity, Integrated Within the Framework

ARTICLE 8

Sits inside the ORM framework and Resilience approach, addressing identification, mitigation, monitoring and ongoing proactive management together.

The Master System of Record must be maintained and stored inside the UAE, including where the underlying activity is outsourced.

Regular testing of mitigating measures, with independent third-party penetration testing required at least for Critical Functions.

A strategy and timeline is required for retiring obsolete, unsupported hardware and software, not solely for the adoption of new systems.

Board and Senior Management must be briefed regularly on ICT and cyber exposure, including incidents and testing results.

Incident Management and Statutory Notification Timelines

ARTICLE 9 & 15

Notify CBUAE	Summary report	High-risk incidents	Confirm normal
4 HRS	**24 HRS**	**72 HRS**	**ON RECOVERY**
The event itself, and which Critical Operations are affected.	Nature of the event, actions taken, likely impact, and timeframe to normal.	Formal notification for any incident classified as high risk under Board-approved criteria.	Notify CBUAE the moment normal operations resume.

Every incident, irrespective of severity, must be recorded in a register capturing its nature, the actions taken and the outcome, the first document auditors and CBUAE examiners are likely to request. (Article 9.4.5)

Risk Data and Systems: Rigour Behind the Reporting

ARTICLE 10

- Risk information systems must deliver the capability and performance required by the institution, including under stressed conditions.
- Governance and internal controls must manage and protect data effectively, For groups, the structure or jurisdiction of subsidiaries and branches cannot be used to justify slow or incomplete risk data aggregation.
- Aggregation and reporting processes are subject to high validation standards and periodic review by Internal Audit.
- The standard for every report, internal or external: comprehensive, accurate, consistent and, above all, actionable.

Business Continuity and Disaster Recovery

ARTICLE 11

Scenarios must span the full range of severity, from recovery with existing assets to the permanent loss of major assets.

Each scenario receives a quantitative and qualitative impact assessment, distinguishing financial, operational, legal and reputational impact.

Plans require clear recovery time and recovery point objectives, reflecting the disruption tolerance the Board has approved.

Tested at least annually for Critical Operations, including key third-party providers where relevant.

Results, together with the plans themselves, are reported to the Board and Senior Management on each occasion.

citadel

VERTEX COMPLIANCE

Extending the Compliance Perimeter

Change management, third-party oversight, Shari'ah risk, disclosure and enforcement.

05

ART. 12 ART. 13 ART. 14 ART. 16 ART. 17

citadel

VERTEX COMPLIANCE

Change Management: a Formal Compliance Gate

ARTICLE 12

Any material change to Critical Operations, or one that could materially affect customers, requires thorough pre-implementation testing and a rollback plan.

An independent external expert must assess the proposed change and the associated controls.

CBUAE must be notified, with that expert's report, at least 30 calendar days before implementation.

Written non-objection from CBUAE is required before the change goes live.

Institutions should incorporate this 30-day lead time into every project plan affecting a Critical Operation, not solely those of a technological nature.

Third-Party Risk Management

ARTICLE 13

1

Guiding principle: institutions must not over-rely on outsourcing, and must retain sufficient in-house staff, expertise and resources to manage the activities for which they are licensed.

2

Risk assessment and due diligence are required before entering any third-party arrangement.

3

CBUAE non-objection is required before outsourcing anything that could significantly affect Critical Operations if disrupted.

4

Contracts must give the institution audit and inspection rights, and CBUAE on-site examination rights where Critical Operations are involved.

5

Exit plans are required, including a candid assessment of the time and cost required to replace a provider.

Shari’ah Non-Compliance Risk: A Concurrent Governance Obligation

ARTICLE 14

Requires a Shari'ah governance framework operating alongside the Operational Risk framework.

Interlinkages between Shari'ah non-compliance and other risks must be understood and tested across the whole life of a contract.

Income not recognised due to non-compliance must be recorded formally and reported regularly to the internal Shari'ah supervision committee.

Separate accounts are required for restricted and unrestricted investment accounts, and for Takaful funds.

Disclosure Obligations and the Enforcement Framework

ARTICLE 16 & 17

DISCLOSURE

- ✓ Public disclosure required on approach to Operational Risk and Resilience, and on Personal Data protection practices
- ✓ Scaled to size, risk profile, complexity and systemic importance
- ✓ Branches and subsidiaries can lean on group disclosures, provided a UAE-specific summary is published too

ENFORCEMENT

- ✓ Fines and administrative or financial sanctions, at CBUAE's discretion
- ✓ Withdrawing, replacing or restricting Board and Senior Management powers
- ✓ Interim management of the institution
- ✓ Barring individuals from the UAE financial sector

Interpretation of the Regulation rests with CBUAE's Regulatory Development Department, not the institution; where ambiguity exists, the more conservative reading should prevail.

Where to Start

A recommended sequencing for the period preceding the effective date.

06

Sequencing Implementation: What to Prioritise

TIER 1 — Now

- Critical Operations mapping (Art. 3.4)[1]
- Risk Appetite & Disruption Tolerance statements
- Incident classification & notification protocols

TIER 2 — 60-90 days

- BCP/DR realignment to new scenarios & RTOs
- Third-party register & re-assessment
- ICT resilience testing programme

TIER 3 — Ongoing

- Change management gate & CBUAE workflow
- Board Operational Risk committee, where required
- Disclosure policy & annual internal control report

1. (Article 3.4)

citadel

VERTEX COMPLIANCE

Where Does Your Institution Stand Right Now?

Score yourself against the three Tier 1 items before we move on. Be honest: "in progress" is not "done."

- [ ] **Critical Operations mapping**
  Do you have a documented map of Critical Operations under Article 3.4, covering people, technology, data, facilities and third parties, and their interdependencies?

- [ ] **Risk Appetite & Disruption Tolerance**
  Are both statements drafted, Board-approved, and reviewed by the same governance forum?

- [ ] **Incident notification protocols**
  Are the 4-hour, 24-hour and 72-hour CBUAE notification triggers written into a procedure, with named owners?

3 of 3
Ready to move to Tier 2 planning.

1–2 of 3
A focused Tier 1 sprint is needed before anything else.

0 of 3
This is the most urgent gap in the room today.

citadel

VERTEX COMPLIANCE

Our Role Across this Implementation Timeline

Regulatory gap assessment

An assessment of the institution's existing framework against all 20 Articles, yielding a prioritised remediation plan.

Critical Operations mapping

Structured support for the Article 3.4 exercise, designed to remain current rather than static.

Change & third-party workflows

Practical design for the CBUAE notification and non-objection processes in Articles 12 and 13.

Ongoing monitoring

Dashboards covering risk appetite, incidents and reporting obligations, ensuring continuous oversight.

citadel

Citadel365's Free Trial



citadel

Join Our WhatsApp Group



citadel

Thank You

www.citadel365.com

info@citadel365.com

+971 56 411 3575

+971 56 496 2986

+971 55 972 7322