

Building a Smarter Customer Risk Assessment Model: Beyond Low, Medium, High



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.

About Us

www.citadel365.com
info@citadel365.com

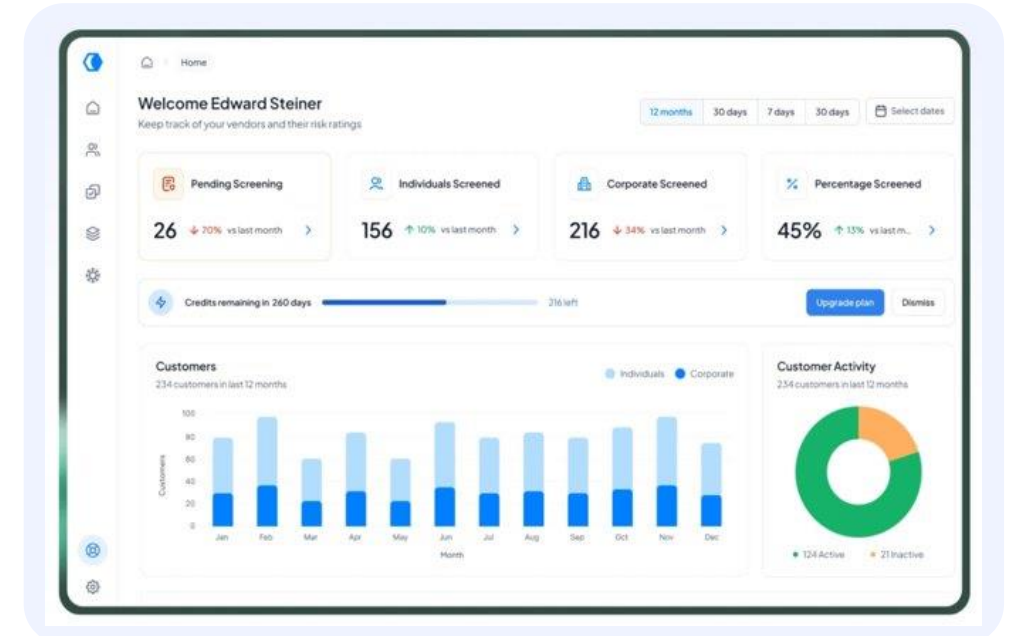
About Citadel365

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.



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.

Outcome

Understand

Meaning of CRA.

It is not a one-time form. It changes when customer risk changes.

Higher risk customers need stronger checks.

The aim is simple: focus resources where risk is highest.

Good CRA protects the business and improves regulatory confidence.

Defining CRA

What is CRA?

CRA is the process of assessing the money laundering, terrorist financing, and proliferation financing risk posed by each customer.

It is conducted at onboarding and updated when risk factors change.

CRA uses customer, geography, product or service, transaction, and channel risk indicators.

CRA outcome determines the level of due diligence, monitoring intensity, and review frequency.

CRA is a core part of the UAE risk-based compliance framework.

Risk-Based Approach: Higher customer risk means deeper checks and tighter monitoring.

There Is No Zero Risk

- ❖ A risk-based AML/CFT framework is not about eliminating all risk. It is about applying **proportionate controls** based on the level and nature of exposure.

- ❖ Every customer and transaction carries some level of risk. The objective is to identify, assess, control, and monitor that risk in a manner that is practical and defensible.

- ❖ Over-controlling low-risk relationships can waste resources, while under-controlling higher-risk relationships creates regulatory and financial exposure.

- ❖ A smart CRA model supports balanced decision-making by matching control intensity to risk.

The Limits of Low, Medium, and High

Many frameworks are too generic and static.

Similar ratings may hide very different risk profiles.

Weak linkage between onboarding CRA and ongoing monitoring.

Manual processes create inconsistency and audit issues.

Supervisory expectations are increasingly outcome-focused, not form-focused.

If two very different customers both land in 'Medium', your controls can become under- or over-calibrated.

UAE Regulatory Anchors for CRA

CRA is not optional in the UAE

UAE framework
requires risk-based
controls and
documented
methodology

CRA should
consider customer,
geography,
product/service/
transaction, and
channel risks

CRA must be
updated periodically
and when trigger
events occur

CRA outcomes drives
CDD/EDD intensity
and review
frequency

In the UAE, CRA is a core compliance control, not a formality.

CRA Vs. ML/FT Risk Assessment

Do not confuse CRA with ML/FT Risk Assessment/IRA/BRA/EWRA/FWRA

- ❖ **CRA:** Risk posed by each customer/prospective customer
- ❖ **ML/FT Risk Assessment:** Enterprise-wide exposure across products, geographies, delivery channels, customers

CRA decisions must align with ML/FT Risk Assessment but stay customer-specific

Both should feed each other through governance and feedback loops

Think of ML/FT Risk Assessment as the map, CRA as the GPS for each customer.

Evolving Towards a Smarter CRA Model

www.citadel365.com

info@citadel365.com

What Smarter CRA Looks Like

From static scoring to dynamic risk intelligence

A smarter model is:

- ❖ **Granular** (not just 3 labels)

- ❖ **Explainable** (why score changed)

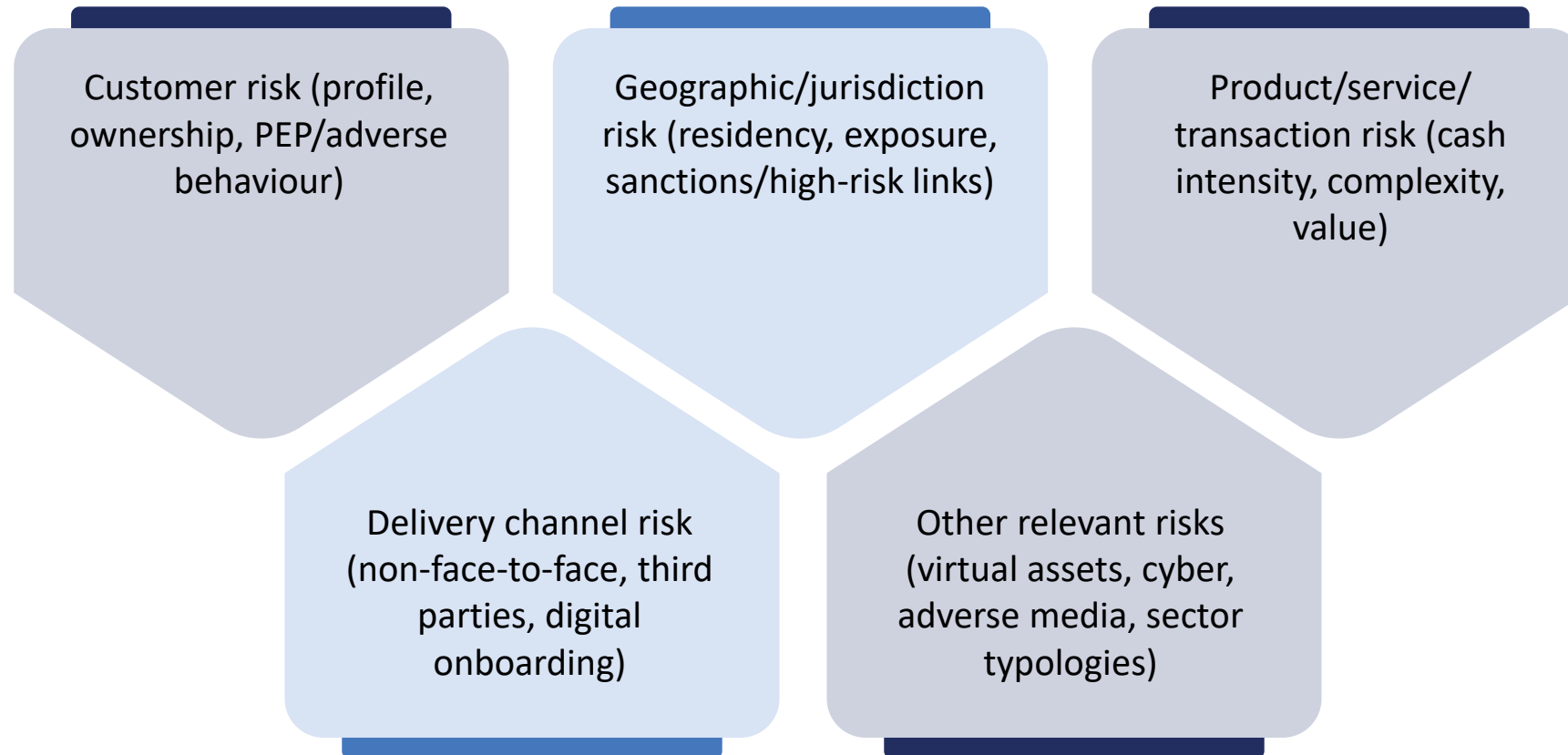
- ❖ **Trigger-based** (real-time updates)

- ❖ **Data-led** (internal + external risk signals)

- ❖ **Action-linked** (CDD/EDD/monitoring tied to risk bands)

Mandatory Risk Factors

Core factors your model must cover:



A Better Risk Scale than 3 Labels

Use bands that improve decision quality

Example rating architecture:

- 1 = Low
- 2 = Low-Medium
- 3 = Medium
- 4 = Medium-High
- 5 = High

Then map to operational actions:

- ❖ KYC depth
- ❖ EDD triggers
- ❖ Approval level
- ❖ Review cycle
- ❖ Transaction monitoring intensity

This creates better prioritisation and fewer false comfort zones.

Risk Scoring Methodology

www.citadel365.com

info@citadel365.com

Weighted Scoring Model

Illustrative weights:

- ❖ Customer profile & behaviour: 30%
- ❖ Jurisdiction exposure: 20%
- ❖ Product/service risk: 20%
- ❖ Transaction pattern risk: 15%
- ❖ Channel risk: 10%
- ❖ External intelligence/adverse media: 5%

Add “hard triggers” that override the score:

- ❖ Sanctions hits
- ❖ Opaque ownership
- ❖ Unexplained third-party funding
- ❖ High-risk jurisdiction
- ❖ Complex structure

Example Risk Scoring Table

Risk factor	Weight	Score range	What pushes score higher
Customer profile and ownership transparency	30%	1 to 5	Complex structures, nominee elements, PEP links, weak transparency
Geography and jurisdiction exposure	20%	1 to 5	FATF high-risk/increased monitoring links, sanctions exposure
Product and service risk	20%	1 to 5	High-value, anonymity-prone, cash-heavy, offshore structuring
Transaction behaviour risk	15%	1 to 5	Unusual patterns, unexplained cross-border flows, third-party funds
Delivery channel risk	10%	1 to 5	Non-face-to-face onboarding without strong digital assurance
Other risk factors	5%	1 to 5	Adverse media, cyber or virtual-asset related risk signals

Overall risk score = Σ (factor score \times weight).

Then map to risk bands and controls.

Turning Scores into Actions

Scoring is useful only if actioned.

Example control mapping:

Band 1–2:

Standard CDD, 24 months refresh

Band 3:

Enhanced monitoring, 12 month refresh

Band 4:

EDD + senior approval, 6 months refresh

Band 5:

EDD+, strict source checks, 3 months/trigger refresh, possible decline/exit

Risk score without action mapping is just decoration.

High-Risk Indicators to Encode in the Model

Red flags your model must capture:

- ❖ Complex ownership with weak transparency
- ❖ Frequent large cash transactions not aligned to profile
- ❖ Non-face-to-face onboarding with weak digital assurance
- ❖ Payments from unknown/unrelated third parties
- ❖ Cross-border activity involving higher-risk jurisdictions
- ❖ Repeated changes in ownership/control with no clear rationale

Trigger Events for Dynamic Re-Rating

CRA should change when risk changes.

Automatic reassessment triggers:

Change in UBO/shareholding/control

Change in business model or products

Unusual transaction behaviour

Sanctions/adverse media developments

NRA/SRA updates or new regulatory guidance

Onboarding through a new channel

Governance and Technology Enablement

www.citadel365.com

info@citadel365.com

Governance Expectations

Who owns what in a smarter CRA model

Board/Senior Management: approves methodology and risk appetite

Compliance/MLRO: policy, calibration, validation, and oversight

Business/Onboarding: data quality and first-line assessment

Internal Audit/QA: independent testing and challenge

Model Governance Forum: periodic tuning and escalation decisions

Common Mistakes in CRA Programmes

What causes weak CRA outcomes:



Technology Stack for Smarter CRA

Minimum viable RegTech architecture

- ❖ Digital onboarding + document verification
- ❖ Rules engine + configurable risk matrix
- ❖ Screening integration (sanctions/PEP/adverse media)
- ❖ Transaction monitoring feedback loop
- ❖ Case management with audit trails
- ❖ Dashboard and reports

How AI/ML Improves CRA

Practical AI/ML use cases (responsibly deployed)

Entity resolution:

better UBO/name matching

Anomaly detection:

behaviour drift vs peer baseline

Graph analytics:

hidden relationships and circular flows

NLP:

adverse media triage and relevance scoring

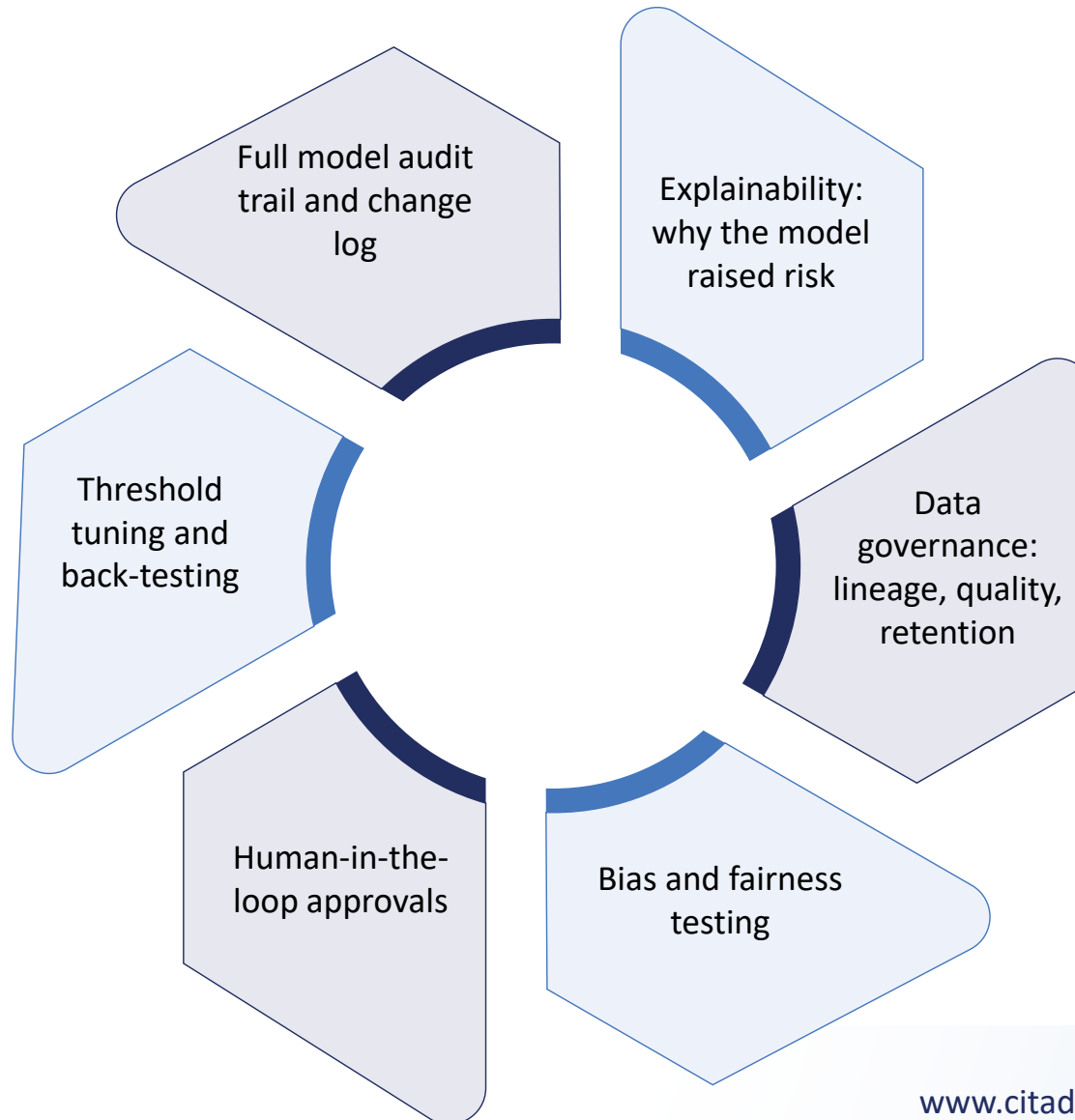
Predictive risk signals:

early warning before incidents

Caution: AI supports decisions; accountable humans make final decisions.

AI/ML Guardrails

Do AI safely and defensibly



Sector Customisation

One CRA model cannot fit every sector.

Financial Institutions:	account behaviour anomalies, third-party deposits, remote onboarding, trade-based money laundering, PEP exposure
Real estate:	beneficial ownership, source of funds, high-value cross-border flows
DPMS:	cash intensity, portability/value concentration
CSP/Trust Services:	complex legal structures, nominee arrangements
Accounting/Legal Services:	client portfolio exposure, service misuse risk
VASP:	wallet/source tracing, typology-led red flags

CRA Model Validation Checklist

Methodology is documented and approved

Risk factors are complete and sector-relevant

Weights are justified and periodically reviewed

Scoring thresholds are clear and practical

Overrides are controlled and evidenced

Data lineage is known and auditable

Trigger events are codified and tested

Output is linked to CDD, EDD, and monitoring

Model results are back-tested against alerts and STR outcomes

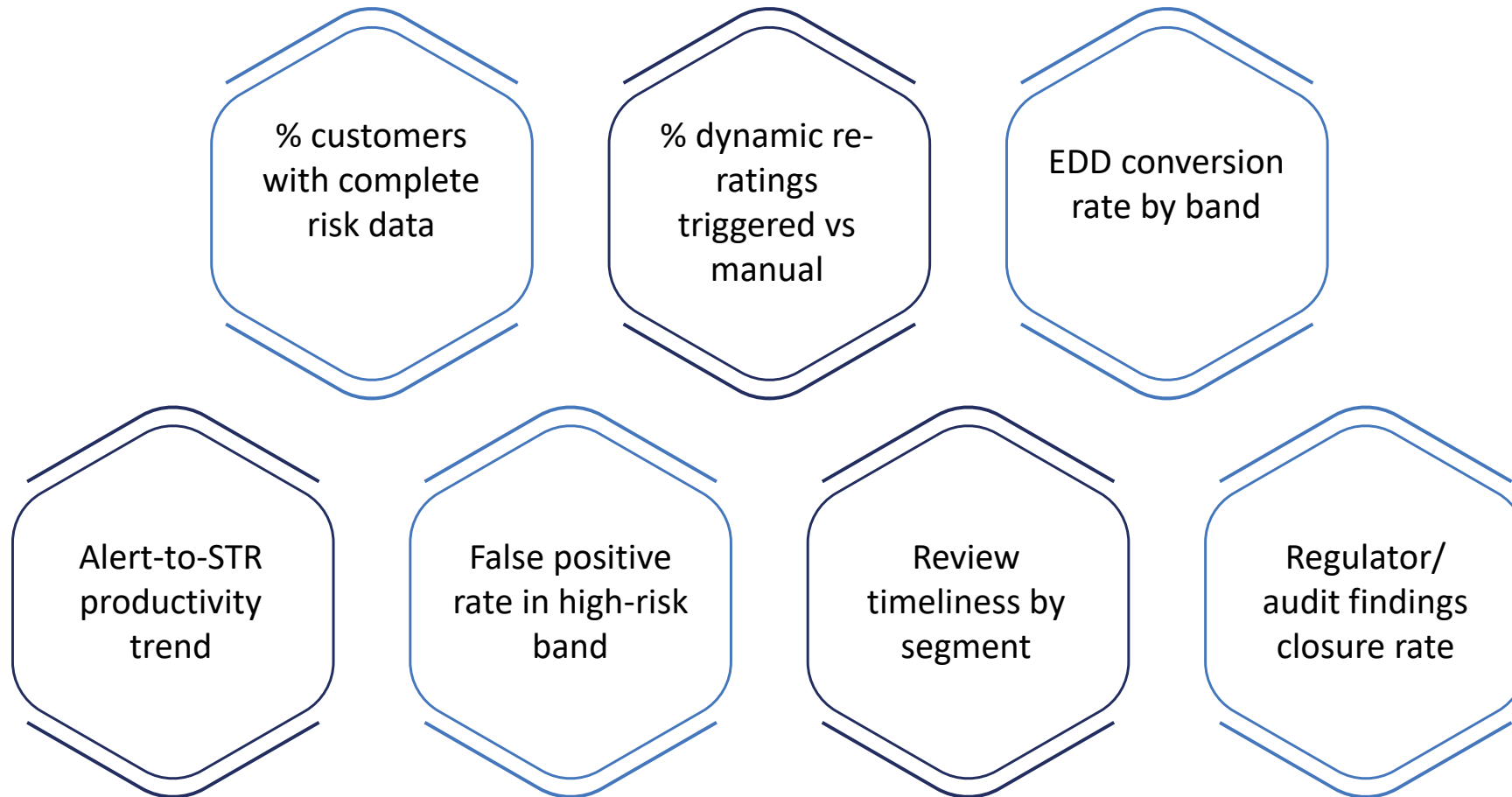
Management information is board-ready

Staff can explain “why this customer is this risk”

Annual review completed, with change log maintained

KPI Dashboard for Management

How to measure CRA effectiveness



Case Study

Same sector, very different risk outcomes.

Customer A and B are both “trading companies”
Traditional model: Both Medium

Smarter model:

A: Clear UBO, local activity, consistent profile → Band 2

B: Layered ownership, third-party inflows, high-risk corridor exposure → Band 4

Outcome: Sharper controls, better resource allocation, stronger defensibility

Quiz

ABC LLC was onboarded six months ago as a Band 2 customer because its ownership appeared straightforward, transaction volumes were expected to remain moderate, and no meaningful adverse media or sanctions concerns were identified at the time of onboarding.

Over the past six months, however, the customer's profile has changed materially. The ownership structure has changed twice, including a transfer involving an offshore shareholder. At the same time, the account has begun showing higher-value and more frequent cross-border transactions connected to a higher-risk jurisdiction, which is inconsistent with the original expected activity profile.

In addition, credible adverse media has surfaced in relation to an associated party, creating further concern about the customer's evolving risk exposure. You are the Compliance Officer assessing what should happen next under a risk-based AML/CFT framework.

What is the best immediate response?

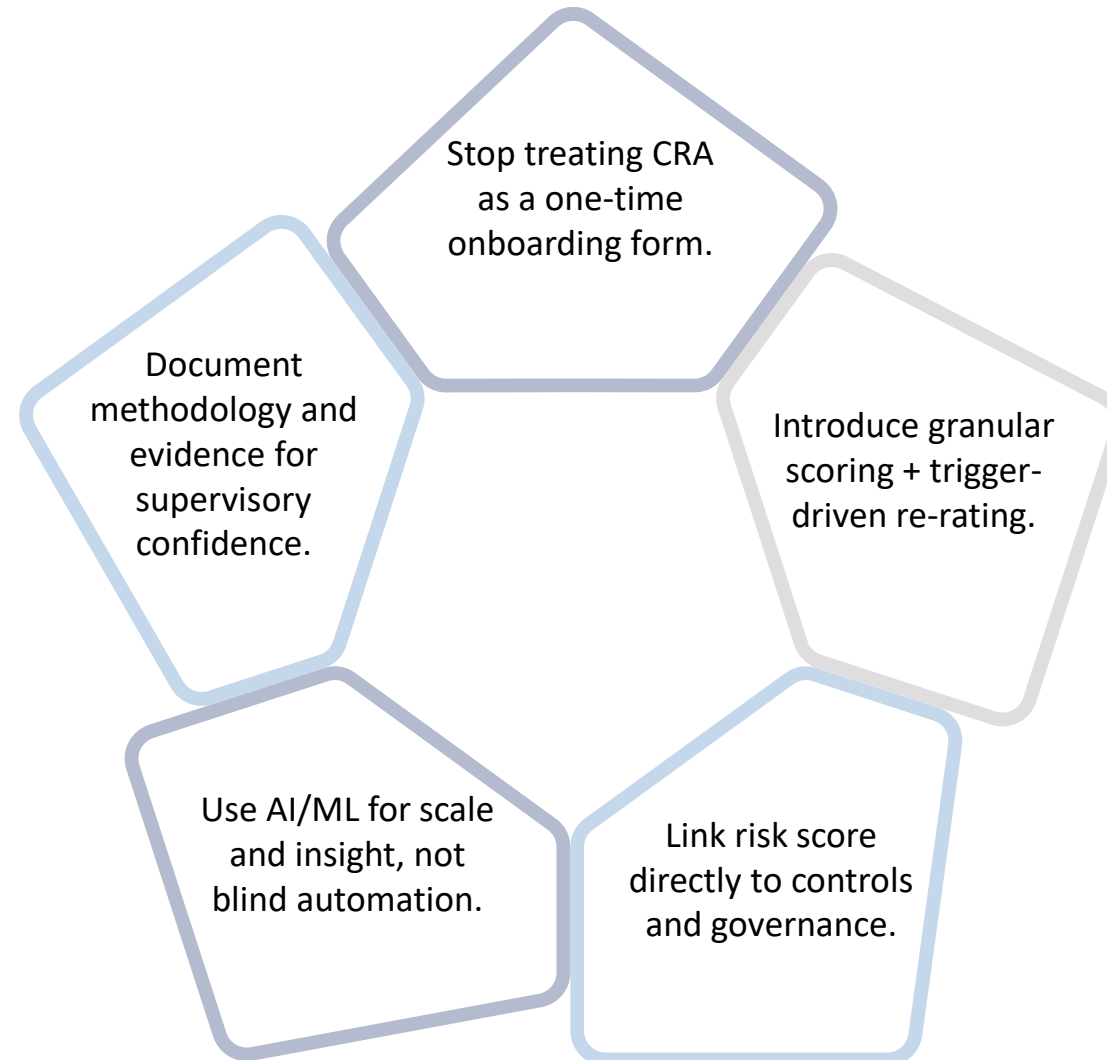
A. Keep annual review cycle

B. Re-rate immediately and apply EDD

C. Wait for transaction alert

D. Ask RM only for verbal comfort

Takeaway



Citadel365's Free Trial



Connect With Us

Join our WhatsApp Group



Thank You



+971 56 411 3575
+971 56 496 2986
+971 55 972 7322



www.citadel365.com



info@citadel365.com