Sanctions & Watchlist Screening: Global Best Practices & Testing Methods

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.

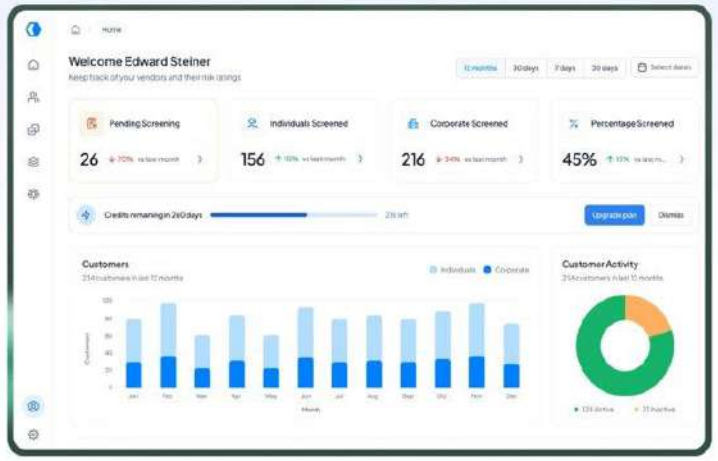
Sridhar Rajam

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

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

Explain global expectations for sanctions and watchlist screening.

Identify critical design elements of an effective screening programme.

Apply robust testing methods to validate controls.

Avoid common mistakes that lead to misses and regulatory findings.

Build a 30-60-90 day improvement roadmap.

Understanding Sanctions Screening

Sanctions Screening

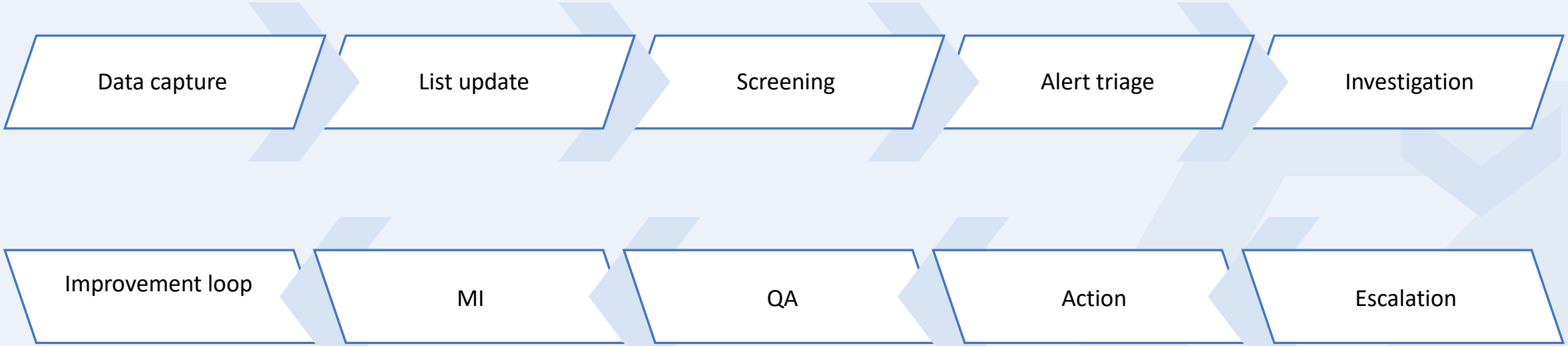
What sanctions screening is

- ✓ A control that checks people, companies, and transactions against sanctions and watchlists.

What it is not

- ✓ It is not a one-click software activity. It is a full process involving data, rules, investigators, escalation, and evidence.

End-to-End Screening Journey



Regulatory Framework for Sanctions Compliance

UAE TFS Operating Framework

UAE TFS compliance is operationally built on four pillars

- ✓ Register for sanctions list updates (EOCN system)
- ✓ Screen relevant parties and transactions
- ✓ Implement TFS measures without delay
- ✓ Report through the prescribed goAML portal

Practical message

- ✓ A screening tool alone is not a full TFS control framework.

CNMR vs PNMR Decision Flow

Step 1: Classify the match

- ✓ Confirmed Name Match
- ✓ Partial Name Match
- ✓ False Positive

Step 2: Apply action

Confirmed match: freeze or reject as applicable, then file CNMR.

Partial match with uncertainty: suspend/restrict as required and file PNMR.

False positive after verification: release with documented rationale and evidence.

Why Screening Failures Still Happen

Common reasons:

Most failures happen because controls are designed in silos:

- ✓ Technology team configures the engine
- ✓ Compliance writes policy
- ✓ Operations handles alerts
- ✓ But end-to-end flow is seldom validated

Global Regulatory Direction

Regulators care about outcomes, not vendor names.

They usually test three questions:

- ✓ Are you screening the right names against the applicable lists?
- ✓ Are you identifying true matches in time?
- ✓ Can you prove your decisions were reasonable and documented?

You are expected to have a process that works under pressure, not just in policy documents.

What Good Looks Like

- Strong governance and accountability
- Timely and quality alert handling
- Risk based list and data coverage
- Algorithms for false positive reductions
- Calibrated matching logic and accurate match percentages
- Management information and board oversight

Designing an Effective Screening Programme

Governance and Accountability Model

- Who approves threshold changes?
- Who can whitelist?
- Who signs off true hit decisions?
- Who informs senior management?
- Who owns remediation deadlines?

Practical tip
If decision rights are not explicit, teams delay escalation and risk grows.

Risk Assessment as Design foundation

- A local low-volume firm and a cross-border high-volume institution should not use identical settings.
- A firm dealing with high-risk jurisdictions needs tighter controls and more frequent refresh.

Design screening based on risk profile:

- ✓ Customer type and ownership complexity
- ✓ Geography and exposure corridors
- ✓ Product and channel risk
- ✓ Nature of transactions
- ✓ Legal and regulatory obligations per jurisdiction

Output:

- ✓ Documented screening scope and rationale

What Must Be Screened

Direct party screening	Indirect party screening	Transactional party screening
(customer)	(UBOs, controllers, signatories)	(originator, beneficiary, intermediaries)

Common misunderstanding to address

“Customer screened at onboarding” does not mean “risk is finished”. New sanctions are issued frequently, so ongoing screening is essential.

Ownership Control and Acting-on-Behalf

Do not assess only legal ownership. Also assess control..

- ✓ Majority ownership thresholds
- ✓ Minority holdings with control rights
- ✓ Acting on behalf of designated parties
- ✓ Authorised signatory or power-of-attorney structures

Sanctions exposure can exist through control or direction, not just shareholding.

Non-Tipping-Off and Staff Conduct

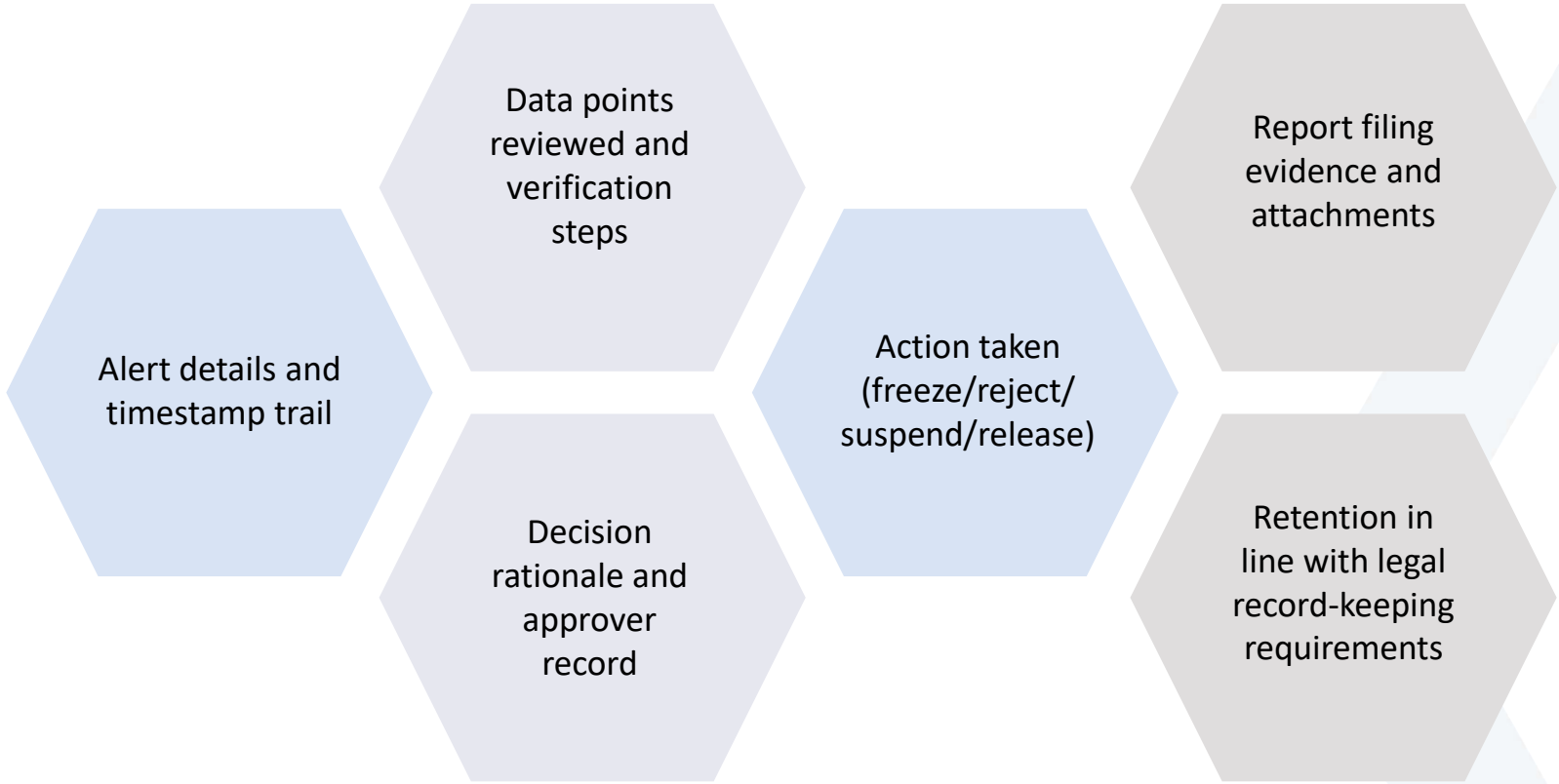
When handling potential or confirmed matches:

- ✓ Do not inform the customer in a way that prejudices controls
- ✓ Restrict internal knowledge to need-to-know staff
- ✓ Use approved communication scripts
- ✓ Escalate sensitive communications to compliance/legal

Operational confidentiality is part of compliance, not optional etiquette.

Record Keeping

Maintain a defensible evidence file for each material alert:



Operational Components of Screening

Data Quality and Entity Resolution

For individuals, capture and validate:

- ✓ Full legal name and known aliases
- ✓ Date of birth
- ✓ Nationality
- ✓ Official ID/passport details

For legal entities, capture and validate:

- ✓ Registered legal name
- ✓ Licence/registration number
- ✓ Jurisdiction
- ✓ Registered and operating address
- ✓ Ownership and control links

Better identifiers mean fewer false closures and stronger true-hit decisions.

Matching Logic and Calibration

Calibration objectives:

- ✓ Maximise detection of true matches
- ✓ Keep false positives manageable
- ✓ Ensure consistency across segments

Methods:

- ✓ Exact match rules
- ✓ Fuzzy match parameters
- ✓ Token and phonetic logic
- ✓ Weighted scoring with threshold bands

Whitelisting and Suppression Controls

Whitelisting is often misunderstood as a productivity shortcut.

It should reduce repetitive known false positives, not suppress risk.

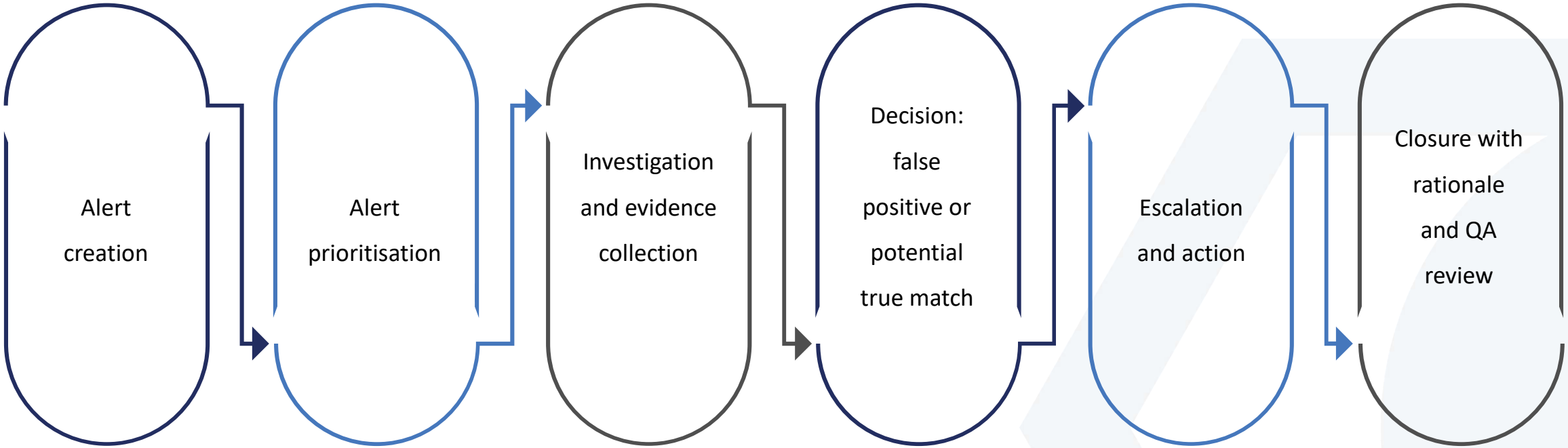
Every whitelist entry needs expiry and periodic review.

Any major sanctions update should trigger whitelist revalidation.

High-risk warning

Permanent whitelists without expiry are a classic control weakness.

Alert Lifecycle and Case Handling



True Match Escalation and Action

Immediate escalation to sanctions compliance

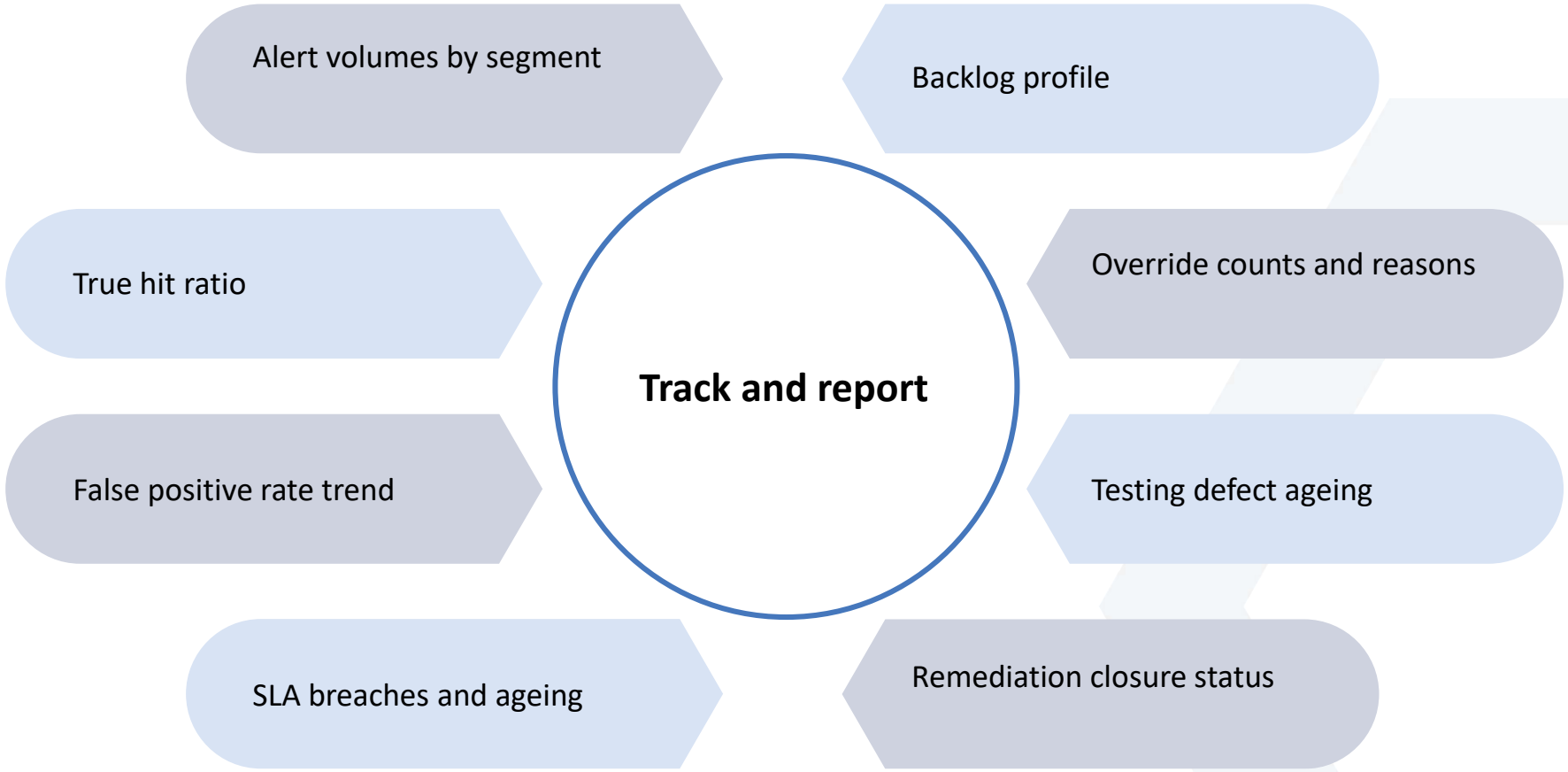
Temporary hold, reject, or block as applicable

Enhanced due diligence on related exposure

Legal and regulatory reporting assessment

Formal decision record and senior sign-off

Management Information and KRIs



Common Challenges and Mistakes

Top Challenges in Practice

Legacy systems cannot always process complex fuzzy rules.

Teams may lack multilingual expertise for complex names.

Sudden sanctions updates can overwhelm operations.

Different jurisdictions may require different handling logic.

Frequent Mistakes to Avoid

- Treating screening as a vendor-only responsibility
- Using default settings without risk calibration
- Ignoring related party and ownership screening
- Weak whitelist governance
- Inadequate testing coverage
- Poor closure documentation
- Delayed remediation of known defects

Strengthening Your Screening Programme

www.citadel365.com info@citadel365.com

30-60-90 Day Improvement Plan

First 30 days

- ✓ Diagnostic review and control mapping
- ✓ Data quality gap assessment
- ✓ Immediate risk fixes for critical defects

First 60 days

- ✓ Calibration refresh
- ✓ Scenario test pack execution
- ✓ Whitelist and exception governance upgrade

First 90 days

- ✓ Independent validation
- ✓ MI and board reporting enhancement
- ✓ Formal remediation closure evidence pack

Scenario 1

A high-risk corporate client clears onboarding screening.

Three months later, an associated controller appears on a new sanctions designation.

Your system did not trigger an alert.

Questions:

What likely failed?

What immediate actions are required?

What control enhancements would prevent recurrence?

Scenario 1

A high-risk corporate client clears onboarding screening.

Three months later, an associated controller appears on a new sanctions designation.

Your system did not trigger an alert.

Questions:

What likely failed?
The failure is in ongoing / delta screening— specifically, trigger-based screening on changes in sanctions lists or related parties

What immediate actions are required?

What control enhancements would prevent recurrence?

Scenario 1

A high-risk corporate client clears onboarding screening.

Three months later, an associated controller appears on a new sanctions designation.

Your system did not trigger an alert.

Questions:

What likely failed?
The failure is in ongoing / delta screening— specifically, trigger-based screening on changes in sanctions lists or related parties

What immediate actions are required? Immediately freeze the account, verify the sanctions match, escalate to compliance, and report to regulators while initiating full rescreening

What control enhancements would prevent recurrence?

Scenario 1

A high-risk corporate client clears onboarding screening.

Three months later, an associated controller appears on a new sanctions designation.

Your system did not trigger an alert.

Questions:

What likely failed?
The failure is in ongoing / delta screening— specifically, trigger-based screening on changes in sanctions lists or related parties

What immediate actions are required? Immediately freeze the account, verify the sanctions match, escalate to compliance, and report to regulators while initiating full rescreening

What control enhancements would prevent recurrence? Implement real-time/event-driven rescreening of all customers and related parties on sanctions list updates.

Scenario 2

Alert volumes dropped by 60 percent after tuning changes.

Operations reported productivity gains.

Two near-match true positives were later identified through manual review.

Questions:

Was this a successful tuning outcome?

Which KRIs should have flagged early warning? Sharp drop in alert volume

How should approvals and rollback be governed?

Scenario 2

Alert volumes dropped by 60 percent after tuning changes.

Operations reported productivity gains.

Two near-match true positives were later identified through manual review.

Questions:

Was this a successful tuning outcome? Over-tuning suppressed sensitivity, causing true positives (near matches) to be missed.

Which KRIs should have flagged early warning?

How should approvals and rollback be governed?

Scenario 2

Alert volumes dropped by 60 percent after tuning changes.

Operations reported productivity gains.

Two near-match true positives were later identified through manual review.

Questions:

Was this a successful tuning outcome? Over-tuning suppressed sensitivity, causing true positives (near matches) to be missed.

Which KRIs should have flagged early warning? Sharp drop in alert volume

How should approvals and rollback be governed?

Scenario 2

Alert volumes dropped by 60 percent after tuning changes.

Operations reported productivity gains.

Two near-match true positives were later identified through manual review.

Questions:

Was this a successful tuning outcome? Over-tuning suppressed sensitivity, causing true positives (near matches) to be missed.

Which KRIs should have flagged early warning? Sharp drop in alert volume

How should approvals and rollback be governed? Sign-off based on documented impact analysis, testing evidence, and risk acceptance. Pre-approved rollback plan with clear triggers, rapid reversion capability, and mandatory post-incident review.

Key Takeaways

- ✓ Screening effectiveness depends on governance, data, calibration, and testing working together.
- ✓ Testing must be periodic, realistic, and independently challenged.
- ✓ Most serious failures arise from preventable mistakes.
- ✓ A structured 30-60-90-day plan can materially improve control maturity.

Stay Updated

Join our WhatsApp Group

citadel

Thank You

+971 56 411 3575
+971 56 496 2986

www.citadel365.com

info@citadel365.com