



The Transaction Monitoring Solution Evaluation Guide

How to assess the Right Transaction Monitoring Solution for
Your Business which improves risk detection and operational
efficiency of compliance teams



Contents

1	Introduction	03
	Transaction Screening and Transaction Monitoring	04
2	What Decision-Makers Will Learn From This Guide	05
3	Define Your Organisation's Monitoring Needs	07
4	Evaluation Area 1: Scenario Alignment With The AML Compliance Programme	12
5	Evaluation Area 2: Payment Data Ingestion	15
6	Evaluation Area 3: Connected Fraud and AML Assessment	19
7	Evaluation Area 4: Risk Scoring and Agentic AI	23
8	Evaluation Area 5: Case Management and Investigation	28
9	Evaluation Area 6: FIU Reporting	32
10	Transaction Monitoring Capability Maturity Matrix	36
11	Measuring Operational Efficiency and Risk Review Improvement	38
12	Measuring Transaction Monitoring Improvement	39
	Transaction Trust Monitoring Solution for Your Business Needs	42

1. Introduction

Businesses need to evaluate transaction monitoring solutions more rigorously as financial crime and fraud typologies evolve and as new financial products carrying greater risk enter the market. The difficulties they face with the solutions already in place are now documented by the institutions operating them.

75%

In a 2025 survey conducted by the American Fintech Council and the Coalition for Financial Ecosystem Standards, 75 per cent of respondents identified transaction monitoring as their single largest compliance expense, citing staffing and system costs. For buyers, this highlights a practical challenge: monitoring teams need to identify meaningful risks while ensuring alert volumes remain manageable enough for effective investigation.

A transaction monitoring solution needs to reflect the risks identified in the firm's AML compliance programme. Its scenarios should align with relevant products, customers, jurisdictions and delivery channels. The solution should also have access to the data required to assess activity in context, support efficient investigation workflows and maintain records that explain decisions and reporting outcomes.

This guide helps decision-makers assess the capabilities required when selecting an AML Transaction Monitoring solution, from risk detection and alert triage to investigation workflows, reporting and operational scalability.

Together, these areas help buyers determine whether a solution can improve monitoring efficiency while supporting risk-based decisions.

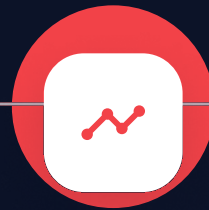
Transaction Screening and Transaction Monitoring

Before evaluating solutions, buyers should establish which control each capability supports.



Transaction screening

Transaction screening evaluates payments against defined restrictions and controls at a specific point in time, such as sanctions requirements or prohibited jurisdiction checks.



Transaction monitoring

Transaction monitoring evaluates activity over time to identify patterns, relationships and behavioural changes that may not be visible from an individual transaction.



2. What Decision-Makers Will Learn From This Guide

Selecting the right AML Transaction Monitoring solution requires evaluating whether it can improve risk detection, reduce operational burden and support better compliance decisions.

This guide helps decision-makers evaluate and choose an AML Transaction Monitoring solution that can help their organisation:

Improve risk detection with better context

Assess whether the solution can combine relevant transaction, customer, identity, fraud and behavioural indicators to provide a more complete understanding of risk.

Increase operational efficiency in alert review

Evaluate whether the solution can reduce unnecessary manual review effort by improving alert triage, prioritisation and access to relevant case information.

Enable confident and explainable risk decisions

Understand whether AML compliance teams can access the evidence behind alerts, review contributing risk factors and make decisions supported by clear context.

Scale monitoring as business requirements evolve

Determine whether the solution can support increasing transaction volumes, new products, customer segments and jurisdictional expansion without creating additional operational complexity.

These assessments are most valuable when applied to the organisation's own monitoring environment. Buyers should therefore begin by defining their current risks, operational challenges and future growth requirements.

3. Define Your Organisation's Monitoring Needs



Transaction monitoring requirements depend on the organisation's business model, sector and growth stage.

A bank operating across multiple jurisdictions, a payment service provider processing high transaction volumes and a marketplace managing seller payouts will each face different financial crime risks, operational challenges and monitoring requirements.

These requirements can also change as organisations expand into new markets, introduce new products, serve new customer segments or experience increasing transaction volumes.

Before selecting a Transaction Monitoring solution, organisations should first define the challenges they need to address. This begins with understanding their risk exposure, current monitoring processes and future business requirements.

Assess the following areas of need:

Alert volumes and review workload

How many alerts are generated today? How many require manual review? Which types of alerts consume the most investigation time?

CONSIDER:

- The volume of alerts generated across products and customer segments.
- The proportion of alerts resolved without further investigation.
- The time AML compliance officers spend reviewing alerts.
- Whether future growth is expected to increase alert volumes.

Business activity changes

How are changes in business activity expected to affect monitoring requirements?

CONSIDER:

- New products or payment methods being introduced.
- Changes in customer behaviour as services evolve.
- New transaction patterns that may create additional financial crime exposure.
- Increased complexity as business operations expand.

Jurisdictional expansion

How will entering new markets affect monitoring requirements?

CONSIDER:

- New customer and transaction risk profiles.
- Different regulatory expectations.
- New payment corridors and counterparties.
- Additional reporting obligations.

Customer segment changes

How do different customer groups create different monitoring needs?

CONSIDER:

- Expected behaviour differences between customer segments.
- Different risk exposure across retail, business or institutional customers.
- Whether current monitoring processes remain suitable as customer populations change.

Sector-specific risk exposure

What financial crime risks are most relevant to the organisation's sector?

FOR EXAMPLE:

- Payment providers may need to consider rapid movement of funds, scam-related activity and linked beneficiary relationships.
- Remittance businesses may focus on corridor risk, repeated sender-beneficiary relationships and structuring patterns.
- Marketplaces may need to assess seller payout behaviour, linked accounts and unusual account activity.

The relevant monitoring requirements depend on the organisation's products, customers, jurisdictions and risk appetite.

Investigation challenges

Where do current investigation processes create operational difficulty?

CONSIDER:

- Time spent collecting information from different systems.
- Difficulty understanding customer, transaction and behavioural context.
- High false-positive volumes creating unnecessary investigation workload.
- Time spent documenting decisions and preparing investigation records.
- Challenges identifying which alerts require further review and which can be resolved efficiently.

Future scalability requirements

How will monitoring requirements change as the organisation grows?

CONSIDER:

- Increasing transaction volumes.
- Additional products and payment flows.
- New customer segments.
- Expansion into additional jurisdictions.
- Growth in investigation workload.
- Changes in alert volumes as business activity increases.

With these requirements documented, buyers can evaluate which Transaction Monitoring capabilities are needed to address current challenges and support future growth.



4. EVALUATION AREA 1

Scenario Alignment With The AML Compliance Programme

The challenge

Monitoring scenarios need to reflect the risks identified by the organisation. When detection logic is not aligned with the AML compliance programme, AML compliance officers may spend significant time reviewing activity that does not require investigation while meaningful risks compete for attention.

The solution should translate the organisation's risk assessment into practical monitoring scenarios.

FOR EXAMPLE:

- A remittance provider may monitor repeated sender-beneficiary relationships, corridor risks and structuring patterns.
- A marketplace may monitor seller payout behaviour, linked accounts and unusual account activity.
- A payment provider may monitor rapid movement of funds and suspicious payment relationships.

The buyer should be able to understand what risk each scenario addresses and how the scenario operates.

Capabilities to assess

- ✓ Prebuilt monitoring scenarios relevant to the organisation's products, customers and markets.
- ✓ Ability to create additional monitoring scenarios.
- ✓ Configuration of thresholds, velocity rules and customer segmentation.
- ✓ Detection of patterns across multiple transactions and linked accounts.
- ✓ Historical testing before deployment.
- ✓ Scenario approval workflows and version history.
- ✓ Mapping between monitoring scenarios and identified risks.

Questions for vendors

- 01 Which AML risks and typologies are covered by your existing monitoring scenarios?
- 02 Can compliance teams configure additional scenarios for new products, customers, jurisdictions or emerging risks?
- 03 Can scenarios be tested against historical transaction data before deployment?
- 04 How are scenario changes reviewed, approved and recorded?
- 05 Can the solution support both prebuilt monitoring scenarios and organisation-specific rule creation?

Scenario Alignment Benchmarks

The standard each capability in this evaluation area should meet.

Scenario coverage

01 Typologies mapped to your risk assessment

Prebuilt scenarios for structuring, smurfing, money mule activity, corridor risk and beneficiary risk, mapped to the enterprise-wide risk assessment

02 Rules written without engineering

No-code, manual and AI-drafted rules, each approved by compliance before activation

03 Every parameter under compliance control

Thresholds, weights, filters, velocity windows and escalation outcomes set by compliance

04 Velocity windows from minutes to months

Short bursts and long-running patterns both covered by configurable time windows

Rule governance

05 Backtested on at least 90 days of history

New or amended rules tested against historical transaction and customer data before deployment, with alert volume and precision recorded for MLRO approval

06 Recalibrated as the business changes

Rules re-tested when products, customer segments or typologies change

07 Every rule version on record

Approver and timestamp recorded for each version, and retained for at least 5 years

Scenario alignment establishes what the solution should detect. The next evaluation area examines whether it receives the information required to perform that assessment.

5. EVALUATION AREA 2

Payment Data Ingestion

The challenge

A monitoring scenario can be well designed but still produce limited insight if payment fields are missing, inconsistent or disconnected from customer information.

AML compliance officers may then spend additional time collecting information before they can understand the activity being reviewed.

The evaluation should consider not only whether a solution can ingest transaction data, but also whether it can interpret the payment information and messaging required to support meaningful risk assessment.

Payment messages contain important details about transactions, including parties involved, payment references, origin and destination information, and other fields that may contribute to identifying suspicious patterns.



Capabilities to assess

- ✓ Support for relevant payment flows and transaction data fields.
- ✓ Ability to ingest and process payment messages relevant to the organisation's operating markets and payment schemes.
- ✓ Support for structured payment messaging formats where applicable.
- ✓ Mapping of payment data and message fields into monitoring scenarios and risk assessments.
- ✓ Connection between transactions, customers, accounts, beneficiaries and related entities.
- ✓ Handling of missing, incomplete or inconsistent payment information.
- ✓ Ability to add new payment sources, message types and data feeds as business requirements change.
- ✓ Scalability to support increasing transaction volumes and additional payment flows.

Questions for vendors

- 01 Which transaction data fields and payment messaging formats can the solution ingest and analyse?
- 02 Can transaction activity be linked with customer, account, beneficiary and related entity information?
- 03 How does the solution use payment message information within risk assessment and monitoring scenarios?
- 04 How does the solution handle missing, incomplete or inconsistent payment data?
- 05 Can additional payment sources, schemes or message formats be added as business requirements change?

Payment Data Ingestion Benchmarks

The standard each capability in this evaluation area should meet.

Transaction data

01 Deep enrichment on every transaction

Payment, device, behavioural, merchant and identity data points available to rules and scoring

02 Payment identifiers captured in full

IBAN, BIC, routing number, card BIN, merchant category code (MCC) and payment method captured with each transaction

03 Non-payment events in the same view

Device, login, account signup and merchant metadata ingested alongside each transaction

04 Business context behind each payment

Company name, merchant ID, industry, MCC, average sales price, currency and sub-merchant data captured

05 Full originator and beneficiary data

Name, account, bank identifier and country captured, with country corridors scored (FATF Recommendation 16)

Rule governance

06 Instant rails monitored through one API

SEPA, FedNow and UK Faster Payments transfers monitored through the same API, with payer, payee and payment fields from the ISO 20022 pacs.008 message mapped to the transaction data (Regulation (EU) 2024/886)

Crypto and data quality

07 Travel Rule data on every crypto transfer

Messages sent and received on the **IVMS 101** standard through **TRP**, **CODE**, **Binance GTR** or direct VASP-to-VASP (FATF Recommendation 16, EU Transfer of Funds Regulation, MiCA)

08 Incomplete data never treated as low risk

Missing or incomplete payer and payee information flagged as "not assessable"

09 A decision on every transaction

Approve, decline or route-to-review returned for each transaction

Integration

10 One API, real time or batch

Decision, risk score, rule hits and evidence returned in one response, connected to core banking, CRM and case management through the API, webhooks and machine-readable exports

11 Historical review in batches

Past transactions submitted in batches for periodic review

12 Monitoring that never pauses

Continuous 24/7 monitoring

Payment data provides the foundation for risk assessment. The next evaluation area examines whether additional fraud and AML signals can contribute to the same risk view.

6. EVALUATION AREA 3

Connected Fraud and AML Assessment

The challenge

Fraud indicators may exist separately from AML monitoring information. When AML compliance officers cannot see the relationship between an account change, device activity and subsequent movement of funds, they have less context for assessing the transaction.

A connected fraud and AML assessment can provide investigators with a unified risk view by bringing together relevant identity, transaction, behavioural and fraud indicators.

This helps teams understand whether activity represents an isolated event or part of a wider pattern involving the customer, account or related entities.

The buyer should test how different signals contribute to the overall risk assessment and how responsibilities are managed across fraud and AML teams.

This is particularly relevant to payment businesses exposed to both scam activity and suspicious fund movement. In the UK, for example, the Payment Systems Regulator's mandatory reimbursement requirements for in-scope Faster Payments authorised push payment scams came into force on 7 October 2024, with a maximum reimbursement level of £85,000 per claim. This illustrates why payment providers may need visibility across both fraud and AML risk indicators. The precise obligations depend on the firm and payment type.

Capabilities to assess

- ✓ Unified risk view combining relevant AML, fraud, identity and behavioural indicators.
- ✓ Identity, customer, device and transaction context available during review.
- ✓ Links between customers, accounts, beneficiaries and related entities.
- ✓ Clear explanation of which signals affected an alert or risk assessment.
- ✓ Defined routes for fraud review, AML investigation and escalation.
- ✓ Integration with existing fraud, KYC and AML systems.
- ✓ Ability to identify patterns across connected entities and transactions.

Questions for vendors

- 01 Which fraud and AML indicators can contribute to the same risk assessment?
- 02 Can investigators view relevant identity, device, behavioural and transaction context together?
- 03 How does the solution identify relationships between accounts, entities, beneficiaries or transactions?
- 04 Can the organisation configure different investigation or response workflows based on the type of risk identified?
- 05 How does the solution distinguish fraud indicators from AML conclusions while allowing both to inform the overall risk assessment?

Connected Screening, Fraud and AML Benchmarks

The standard each capability in this evaluation area should meet.

Fraud and AML signals

01 One score for fraud and AML

KYC outcome, AML screening, fraud signals and transaction monitoring resolved on one platform into one composite risk score

02 Linked accounts surfaced automatically

Shared email, phone, IP, device, payment identifiers or beneficiaries flag mule behaviour that doesn't fit the verified identity

03 Device and location risk in every score

Device mismatch, account takeover behaviour, velocity spikes and new-recipient risk assessed alongside IP geolocation and VPN, TOR and proxy detection

04 Every alert tied to the verified identity

Each alert linked to the customer's KYC outcome, screening status and risk rating (FATF Recommendation 10)

Sanction screening

05 Every major regime, every entity type

OFAC SDN, UN Security Council, EU Consolidated, UK, DFAT and SECO lists across individuals, entities, vessels, aircraft and crypto wallets, with OFAC 50 Percent Rule resolution and its EU and UK equivalents and major sanctions regimes across the globe

06 Lists refreshed within minutes, not daily

Enrolled customers re-screened each cycle, well inside the daily screening the EU Instant Payments Regulation requires for **SEPA Instant** (Article 5d, Regulation (EU) 260/2012 as amended by Regulation (EU) 2024/886)

07 Both parties screened in one request

Customer and beneficiary screened against sanctions, PEP and adverse media filters in the same transaction request

PEP, watchlist and crypto screening

08 PEP coverage down to local officials

PEPs tiered in line with FATF guidance, including local and municipal officials, with relatives and close associates linked and given the PEP's tier (FATF Recommendation 12)

09 Global watchlists and multilingual adverse media

Thousands of watchlists, adverse media monitored across languages and risk categories, and internal lists screened with the same matching logic

10 Results in seconds, every decision explained

Fuzzy, phonetic and transliteration matching with a configurable threshold, and AI-assisted Level-1 triage that gives a reason for each decision

11 Counterparty VASPs checked before data is sent

Each VASP risk-scored, with KYB status and MiCA authorisation checked before Travel Rule data is sent, and unhosted wallet ownership verified by Satoshi test, signature proof, visual proof or self-declaration

Connecting signals improves the context available for review. The next evaluation area examines how that context is used to prioritise alerts and support AML compliance decisions.

7. EVALUATION AREA 4

Risk Scoring and Agentic AI

The challenge

Many vendors position AI capabilities around reducing alert volumes and improving investigation efficiency. These outcomes can be valuable, but buyers should examine how the reduction is achieved.

A lower alert count may result from better contextual assessment and appropriate resolution of lower-risk activity. However, it may also reduce visibility into activity that requires investigation if the alert resolution mechanism does not consider the right risk indicators.

Buyers should therefore understand how the solution determines which alerts can be resolved, which require further review and which should be escalated.

The assessment should consider the evidence available, the risk indicators evaluated and whether the outcome follows the organisation's AML compliance programme.

Risk scoring and Agentic AI can support AML compliance officers by bringing together customer, transaction, identity, fraud and behavioural context. This can help teams prioritise alerts, reduce repetitive review work and focus attention on activity requiring further investigation.

Capabilities to assess

- ✓ Risk scores based on relevant transaction, customer and behavioural indicators.
- ✓ Contextual alert assessment using identity, AML, fraud and other risk signals.
- ✓ Alert prioritisation based on risk exposure and compliance rules.
- ✓ AI-assisted alert summaries and investigation support.
- ✓ Visibility into evidence and factors contributing to risk assessments.
- ✓ Defined criteria for alert resolution, further review and escalation.
- ✓ Human review controls where required by the organisation's compliance programme.
- ✓ Audit history of decisions, overrides and workflow changes.
- ✓ Scalability of risk assessment as transaction volumes, products and jurisdictions increase.

ALERT ASSESSMENT
PRIORITISED

Risk score and contributing factors

TRANSACTION

CUSTOMER

BEHAVIOURAL

AI-ASSISTED ALERT SUMMARY
READY

HUMAN REVIEW
REQUIRED

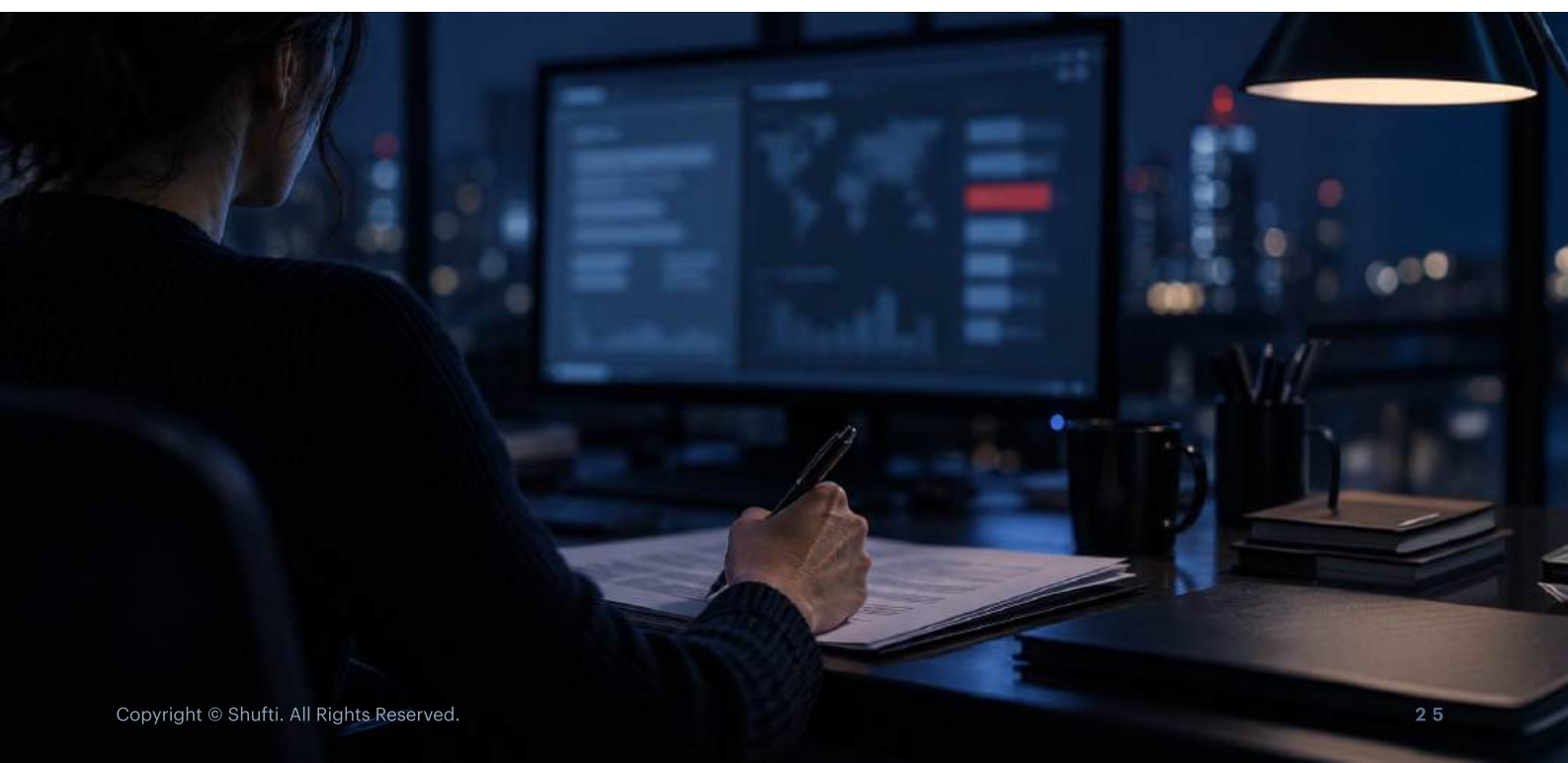
Resolve

Further review

Escalate

Questions for vendors

- 01 How does the solution determine the risk level of an alert?
- 02 Which data points contribute to the risk assessment?
- 03 Can an AML compliance officer understand why an alert was prioritised, resolved or escalated?
- 04 How does the solution differentiate between alerts that can be resolved efficiently and those requiring further investigation?
- 05 How does the workflow handle missing, conflicting or insufficient information?
- 06 Can compliance teams review, challenge and approve recommendations before final action?
- 07 How are decisions, overrides and changes recorded for future review?
- 08 How does the solution maintain consistent risk assessment as transaction volumes and business requirements increase?



Risk Scoring and Agentic AI Benchmarks

The standard each capability in this evaluation area should meet.

Risk scoring

01 One composite risk score per transaction

Alerts routed to L1, L2 or MLRO by risk level

02 Crypto wallets rated by risk

Wallets classified Low, Medium or High against sanctions lists, watchlists and frozen-address lists, with an audit-ready report and each wallet hit linked to a verified identity

03 Every risk factor visible

Each contributing signal shown and marked as raising, lowering or neutral to risk

04 Customer context in every score

KYC status, account age, risk rating, source of wealth, screening outcome and prior decisions feed each transaction score

05 Behaviour compared with the customer's own baseline

Amount, frequency, timing, device and transaction type compared against each customer's own recent history

Alert Quality

06 Fewer false positives, proven on your data

A measurable reduction in false positives against the current baseline, shown on the buyer's own data

07 Suppression with an audit trail

Repeat low-risk patterns suppressed only under documented conditions, and every suppressed decision stays auditable

08 Low friction for good customers

Low-risk transactions approved in real time, and recurring safe patterns do not trigger repeat reviews

AI governance

09 Every score explained and reproducible

Each alert shows the rules triggered and contributing signals

10 AI tested for bias

AI models tested for bias, with hybrid AI and human review so automated outcomes are checked by compliance before they become final

11 Compliance keeps the final say

AI drafts and recommends, compliance approves, and every override is logged

Prioritisation creates value when it helps AML compliance officers reach and document better decisions. Buyers should therefore evaluate how effectively those decisions move into investigation workflows.



8. EVALUATION AREA 5

Case Management and Investigation

The challenge

An alert may contain a risk score but still leave an AML compliance officer searching across multiple systems for customer information, transaction history, previous alerts and related risk indicators.

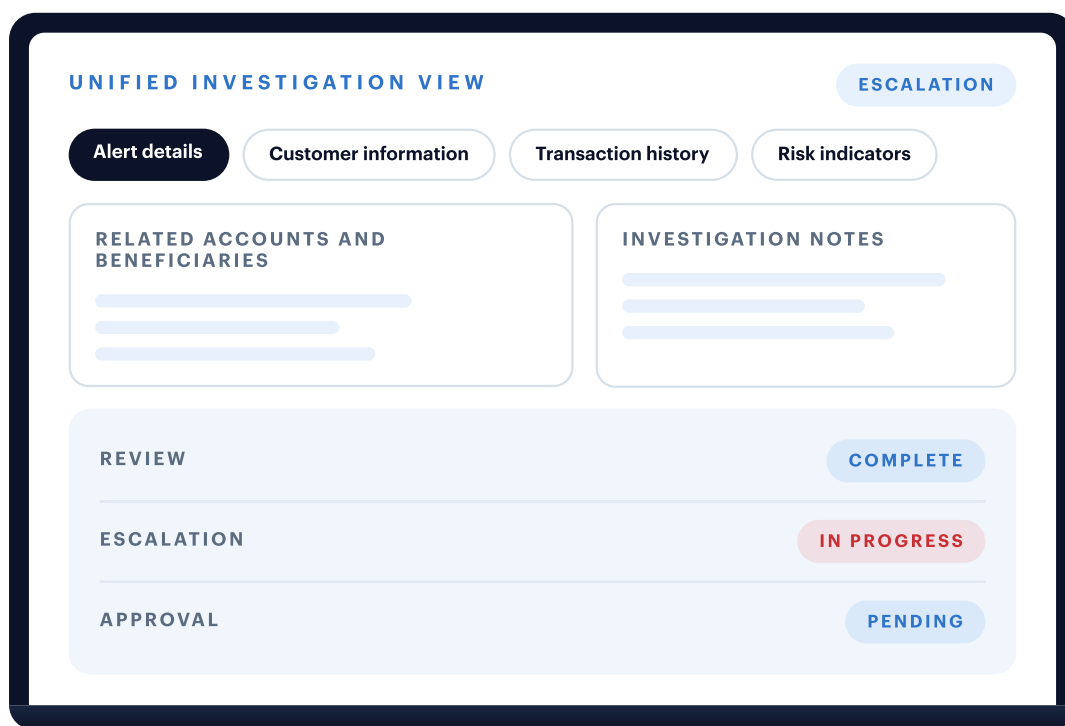
This creates additional review effort and makes it harder to build a complete understanding of the activity being investigated.

A strong case management workflow should provide a unified risk view by bringing together relevant customer context, transaction activity, risk indicators, investigation history and previous decisions.

This allows investigators to spend less time reconstructing information and more time assessing the activity requiring judgement.

Capabilities to assess

- ✓ Unified investigation view combining alert details, customer information, transaction history and relevant risk indicators.
- ✓ Access to the scenarios and factors that triggered the alert.
- ✓ Visibility of related accounts, beneficiaries and linked activity where relevant.
- ✓ Integration of identity, fraud, behavioural and transaction context.
- ✓ Investigation notes and evidence retained with the case.
- ✓ Configurable review, escalation and approval workflows aligned with the organisation's operating model.
- ✓ Recorded decisions, overrides, approvals and timestamps.
- ✓ Searchable audit history and support for quality assurance reviews.
- ✓ Ability to support increasing investigation volumes across teams, products and jurisdictions.



Questions for vendors

- 01 Can investigators view the complete context behind an alert in one place?
- 02 Which customer, transaction, identity, fraud and behavioural signals are available during investigation?
- 03 Can investigators see related activity, accounts or entities connected to the case?
- 04 Can investigation teams assign, track and manage cases according to their internal processes?
- 05 Can cases be escalated when additional review or approval is required?
- 06 Can reviewers understand what information was considered, what actions were taken and why a decision was reached?
- 07 Are investigation notes, decisions, approvals and changes recorded for audit purposes?
- 08 Can the case history support regulatory reviews, internal quality checks or future investigations?
- 09 Can the workflow support increasing investigation volumes as the business expands?

Case Management and Investigation Benchmarks

The standard each capability in this evaluation area should meet.

Alert handling

01 Alerts routed by risk and context

Routed by risk score, typology, jurisdiction, customer tier and data completeness

02 A clear escalation path

L1 to L2 to MLRO, with four-eyes review and SLA tracking

03 Evidence assembled before review

Rule trigger, score explanation, linked accounts, behavioural deviation and adverse media gathered before an analyst opens the case

04 Investigation checks run in parallel

Investigation agents check pattern history, screening context, device and IP, receiver networks and prior cases at the same time

Rule governance

05 Cases exported in machine-readable formats

Narrative, linked entities, decision history, analyst notes, rule metadata and score explanations exported for audit, regulator requests and downstream compliance systems

06 Records retained for at least 5 years

Actions, decisions and closure rationale kept on record (31 CFR 1010.430; UK MLRs 2017 reg. 40)

A complete investigation record also supports reporting decisions. The next evaluation area examines whether that information can flow into applicable FIU reporting processes.

9. EVALUATION AREA 6

FIU Reporting

The challenge

SAR Reporting requirements depend on the jurisdiction, report type and activity involved. When case information has to be re-entered or reconstructed, investigators and reporting officers face additional work and a greater risk of omissions.

The solution should carry relevant customer, transaction and investigation information into applicable reporting workflows while supporting review and approval under the organisation's procedures.

Vendor support should be assessed against the financial intelligence units (FIUs) and report types relevant to the organisation, including SARs, STRs or other regulatory reports where applicable.

Specific instructions illustrate why this matters. In a US alert concerning virtual currency investment scams, FinCEN requests that filers include a named key term in SAR field 2 and the narrative when filing in connection with that alert. UKFIU guidance separately explains how relevant glossary codes and NCA Alert codes should be used in applicable UK SARs. These are jurisdiction-specific examples of reporting guidance. Buyers should test support for the instructions relevant to their own filings.

Capabilities to assess

- ✓ Support for relevant FIU formats, fields and reporting workflows.
- ✓ Transfer of case facts and evidence into report preparation.
- ✓ Review and amendment of structured fields and narrative.
- ✓ Support for applicable references, codes or alert terms where required.
- ✓ Internal review and approval workflows.
- ✓ Submission status, amendments and audit records.
- ✓ Ability to maintain reporting records linked to the underlying investigation.

Questions for vendors

- 01 Which FIU formats and reporting workflows does the solution support for the jurisdictions relevant to the organisation?
- 02 Can investigation information flow into report preparation without requiring teams to rebuild the case manually?
- 03 Can compliance teams review, edit and approve reports before submission?
- 04 Can the solution support relevant reporting instructions, codes or references where required?
- 05 Are reporting decisions, approvals, submissions and amendments recorded?
- 06 How are reporting requirements updated when regulatory expectations change?

FIU Reporting Benchmarks

The standard each capability in this evaluation area should meet.

Filing

01 Direct FinCEN e-filing

Submission through the BSA E-Filing System in BSA XML 2.0, with the acknowledgement captured (accepted, accepted with warnings, rejected)

02 SARs filed on time

FinCEN SARs filed within 30 calendar days of initial detection (60 where no suspect is identified), with a deadline tracker escalating before the window closes (31 CFR Chapter X)

03 CTRs batched automatically

Cash transactions over USD 10,000 per business day batched and filed within 15 days, with every pause logged with a reason (31 CFR 1010.311, 1010.306)

04 goAML filing across FIUs

Native goAML XML submission with validation receipts tracked, and further goAML FIUs added largely by configuration

05 Reports pre-filled from the evidence

Narrative and suspicious indicators drafted from the fired rule and linked evidence, with subject identity locked to the verified KYC record

Oversight and records

06 No SAR files without the MLRO

Every SAR and STR approved by the MLRO before submission, returns need a recorded reason, and only CTRs file automatically

07 A plain-English view of every filing

Each filing shown in plain English, with the exact submitted XML one click away

08 FIU follow-up tracked

Information requests tracked with due dates, and rejected filings corrected and re-filed on the same record

09 Filings retained for 5 years

Filings, approvals and FIU responses kept, with the submitted XML retrievable (31 CFR 1020.320(d))

The six evaluation areas provide a structured way for buyers to assess Transaction Monitoring solutions. The following maturity matrix helps organisations identify their current capability level and understand which capabilities they need to evaluate next.

10. TRANSACTION MONITORING CAPABILITY MATURITY MATRIX

Transaction Monitoring Capability Maturity Matrix

Organisations may have capabilities across multiple maturity levels depending on their current operating model, risk exposure and growth stage.

This framework helps buyers identify where their current challenges exist and which capabilities they should evaluate when selecting a Transaction Monitoring solution.

MATURITY LEVEL	BUSINESS CHALLENGE	CAPABILITIES TO ASSESS
LEVEL 1: Rules-Based Transaction Monitoring	AML compliance teams rely on predefined scenarios and thresholds. Adapting monitoring coverage for new products, markets or financial crime typologies requires significant manual effort or technical support.	Prebuilt AML rules library, scenario configuration, threshold management, rule creation, scenario testing, approval workflows and alert generation.
LEVEL 2: Risk-Based Transaction Monitoring	Monitoring scenarios do not consistently reflect the organisation's AML compliance programme, risk appetite or changing business requirements.	Alignment with enterprise-wide risk assessment, customer and product segmentation, jurisdictional risk assessment, behavioural monitoring, scenario calibration, approval workflows and version history.

MATURITY LEVEL	BUSINESS CHALLENGE	CAPABILITIES TO ASSESS
LEVEL 3: Contextual Transaction Monitoring	AML compliance officers spend significant time gathering customer, identity, payment and behavioural information before assessing alerts. Relevant signals may exist across different systems, limiting the ability to understand the complete risk picture.	Unified risk view, customer and account history, payment data, payment messaging, beneficiary information, identity context, device intelligence, behavioural indicators, linked activity and connected fraud and AML assessment.
LEVEL 4: AI-Assisted Risk-Based Transaction Monitoring	AML compliance teams need to prioritise meaningful risks, reduce repetitive review work and support better decisions while maintaining evidence, governance and control over AI-assisted recommendations.	Explainable risk scoring, Agentic AI-assisted alert triage, evidence-backed recommendations, contextual alert summaries, configurable workflows, human review controls, investigation management and audit trails.
LEVEL 5: Scalable Transaction Monitoring Operations	Organisations expanding across products, customer segments and jurisdictions need monitoring capabilities that can grow with business complexity without creating disproportionate alert volumes, review effort or operational challenges.	Operational scalability across transaction volumes, products and jurisdictions; support for new payment flows and data sources; flexible monitoring architecture; scalable investigation workflows; consistent risk assessment across markets; governance controls for expanding monitoring operations.

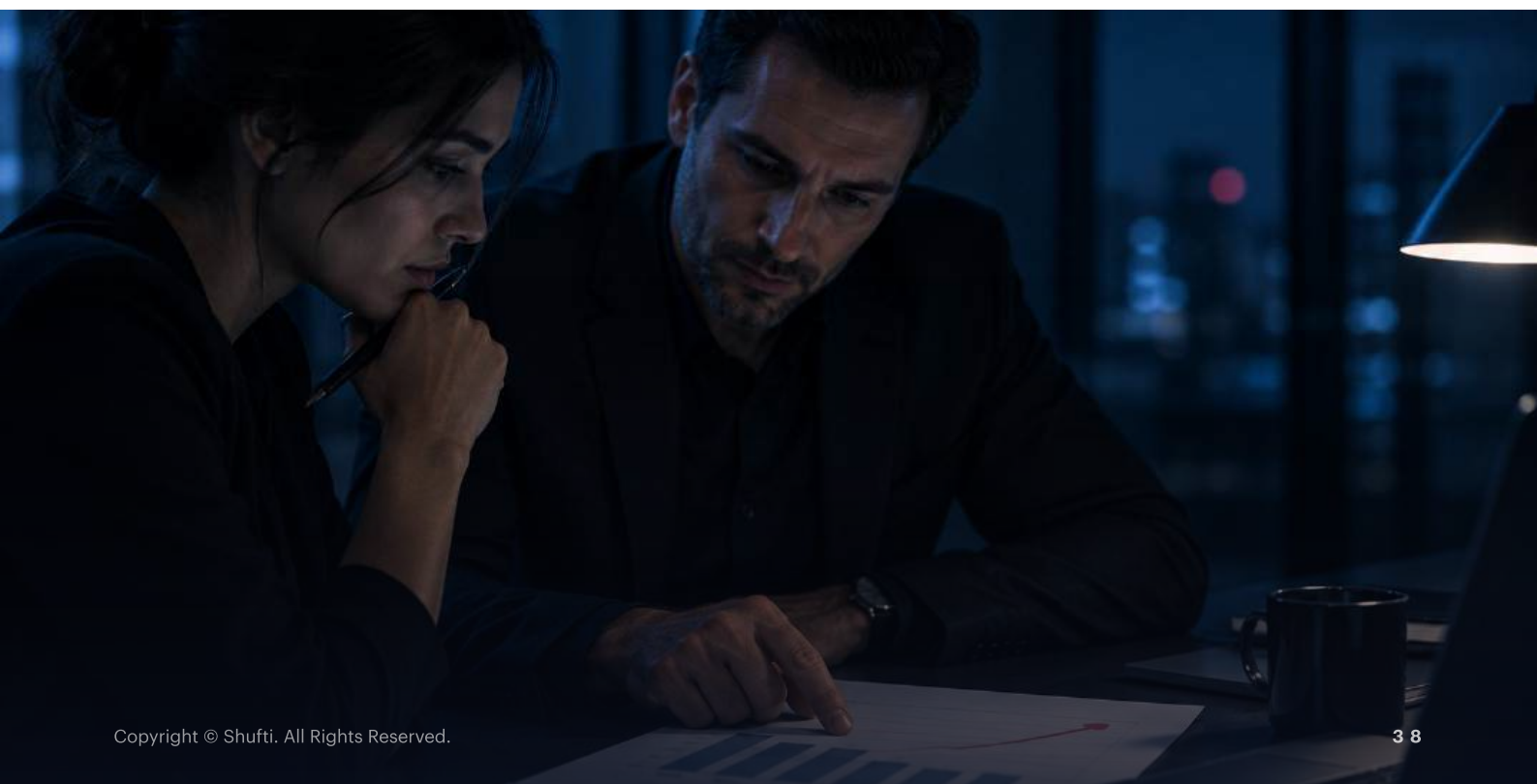
11. Measuring Operational Efficiency and Risk Review Improvement

The challenges identified throughout this guide directly affect two outcomes decision-makers need to evaluate when selecting a Transaction Monitoring solution:

- **Whether the solution reduces the manual effort required to review alerts.**
- **Whether it helps AML compliance teams focus more review capacity on actual risks which require investigation**

A reduction in alert volumes alone does not demonstrate improved monitoring. Buyers should evaluate whether efficiency improvements result from better risk assessment, stronger alert triage and access to relevant context.

The following calculations help estimate how a new Transaction Monitoring solution may improve operational efficiency while maintaining focus on meaningful risks.

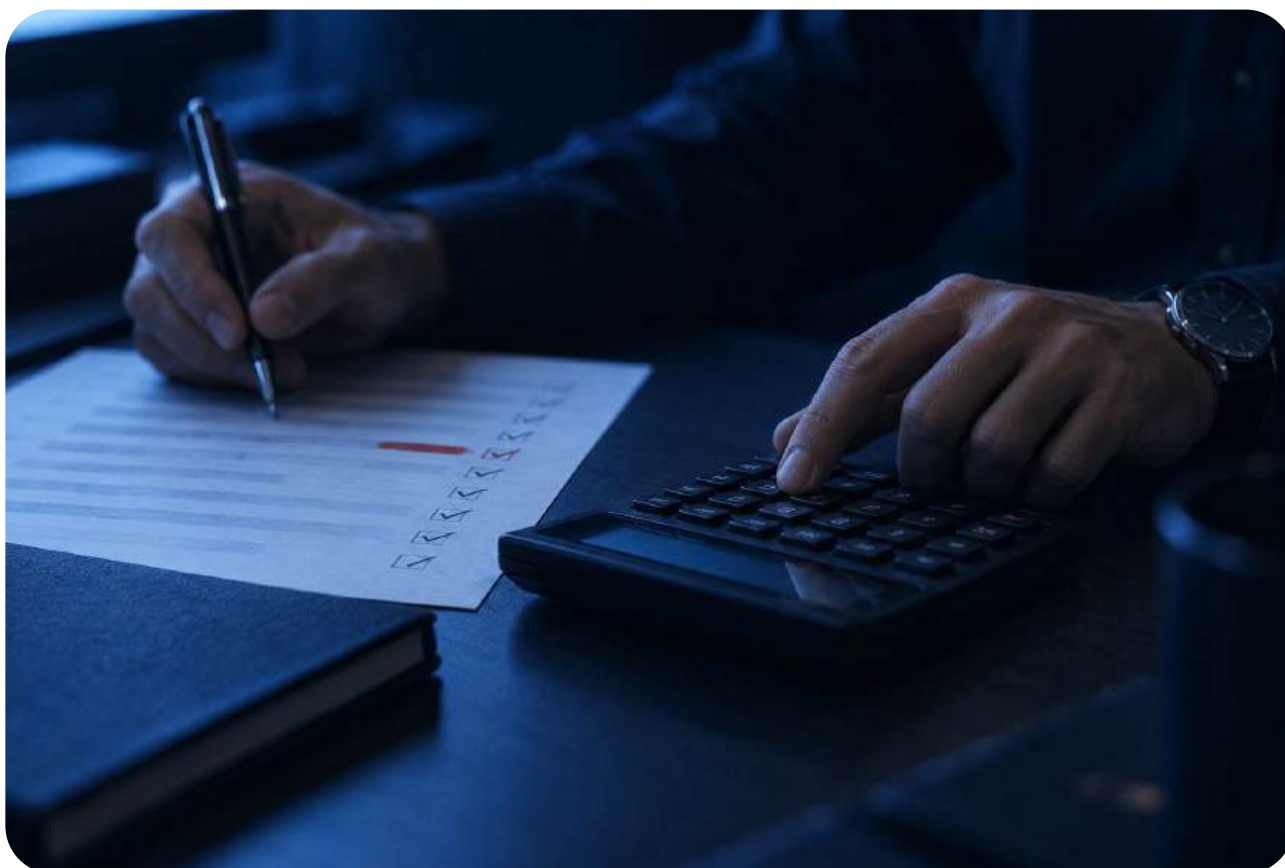


12. Measuring Transaction Monitoring Improvement

A Transaction Monitoring solution should help organisations address two core challenges:

- Reducing the manual effort spent reviewing alerts that do not require further action.
- Improving the focus of compliance teams on alerts that represent relevant risks.

This calculator helps buyers evaluate how reducing false positives can improve operational efficiency and increase the proportion of review effort directed towards meaningful risk.



1. Operational Efficiency Improvement

Purpose

Measures the reduction in manual alert review effort achieved through a reduction in false positive reviews.

Formula

Operational Efficiency Improvement (%)

$$= \frac{\text{Reduced False Positive Review Hours}}{\text{Current Total Manual Review Hours}} \times 100$$

Reduced False Positive Review Hours

$$= \text{Number of False Positive Alerts Reduced} \times \text{Average Review Time per Alert}$$

Current Total Manual Review Hours

$$= \text{Total Alerts Reviewed} \times \text{Average Review Time per Alert}$$

Required Inputs

- ✓ Total alerts reviewed annually
- ✓ Average review time per alert
- ✓ Number of false positive alerts reduced

2. Relevant Risk Detection Improvement

Purpose

Measures how reducing false positive reviews can increase the proportion of compliance review capacity focused on alerts that require investigation.

Formula

Relevant Risk Detection Improvement (%)

$$= \frac{\text{Additional Relevant Risk Alerts Reviewed}}{\text{Current Relevant Risk Alerts Reviewed}} \times 100$$

Additional Relevant Risk Alerts Reviewed

=

$$\text{Reduced False Positive Alerts Available for Risk Review} \times \text{Relevant Risk Identification Rate}$$

Current Relevant Risk Alerts Reviewed

=

$$\text{Current Alerts Reviewed} \times \text{Current Relevant Risk Identification Rate}$$

Transaction Trust Monitoring Solution for Your Business Needs

Financial crime risks evolve as businesses grow. New products, payment flows, customer segments and jurisdictions introduce new monitoring requirements, while existing teams continue to manage alert volumes and investigation complexity.

Transaction Trust Monitoring helps organisations build a more adaptive approach to transaction monitoring — from establishing coverage with pre-built risk scenarios to configuring rules that reflect their specific products, customers and risk exposure.

Shufti's Transaction Trust Monitoring Against the Benchmarks in This Guide

How Shufti Transaction Trust Monitoring meets each evaluation area in this guide, with every decision anchored to the customer's verified identity.



Identity Context

Every transaction scored against fraud and AML rules tied to the verified identity behind the account. KYC outcome, screening status, customer risk rating, source of wealth, device context and transaction behaviour resolve into one composite FRAML risk score. KYC, AML screening and transaction monitoring run on one platform, and reports carry verified identity and liveness-backed onboarding context.



Scenario Alignment and Rule Builder

No-code rule builder aligned to your AML compliance programme. Start from typology rules for structuring, smurfing, mule activity, corridor and beneficiary risk, or draft rules with the AI wizard. Compliance sets thresholds, weights, filters, velocity windows from 1 minute to 6 months and escalation outcomes. Every rule is backtested on a minimum of 90 days of history and approved before deployment, with full version history.



Payment Data Ingestion

1,600+ data points per transaction. One REST API for real-time and batch. 24/7 monitoring.



Case Management

L1 to L2 to MLRO escalation with four-eyes review and SLA tracking. Parallel investigation agents. Records kept for at least 5 years.



Crypto and Travel Rule

VASP-to-VASP flows identified automatically, with Travel Rule data sent and received on IVMS 101 through TRP, CODE and Binance GTR. Counterparty VASPs scored from 1 to 100. Wallets screened against 215+ sanctions lists and 4,000+ watchlists, rated Low, Medium or High, with every wallet hit linked to the verified customer who owns it.



FIU Reporting

Direct filing to US FinCEN in BSA XML 2.0. goAML-ready across jurisdictions, including the UAE, Pakistan, India, Nigeria and Iraq. Report-ready case bundles with subject details, transaction chronology, triggered typologies and analyst rationale. The MLRO approves every SAR and STR before submission.



Screening, Fraud and AML

215+ sanctions regimes, refreshed every 15 minutes. 2.6M+ PEP profiles in four tiers. 4,000+ watchlists from 100,000+ sources. Adverse media in 80+ languages across 415+ risk categories. Results in under 3 seconds on average.



Deployment and Security

SOC 2 Type II, ISO/IEC 27001:2022, PCI DSS AoC and Cyber Essentials Plus. SaaS, private cloud or on-premise deployment. Processing regions in the EU, UK, US, APAC and MENA. Sandbox within 24 hours and API integration in 2 to 5 business days.



Risk Scoring and Agentic AI

Up to 60% fewer false positives. An AI agent clears up to 60% of Level-1 triage. 90-day behavioural memory.



Give Your Team Fewer Alerts to Review

Bring Customer Context Into Every Transaction Risk Assessment.

Reduce manual alert review effort by up to 60% so your team can focus on unusual transaction behaviour and connected activity that needs investigation.

Shufti's Transaction Trust Monitoring combines transaction data, customer identity and AML signals in one integrated FRAML view. It assesses multiple data points against scenario typologies to identify suspicious patterns, while agentic AI supports alert triage and helps teams prioritise investigations.

[Explore Transaction Trust Monitoring](#)

Shufti is based in the United Kingdom and operates offices worldwide.



United States

16200 SW Pacific Hwy,
Suite H PMB 1053,
Tigard, OR



Cyprus

Arch. Makarios III
Avenue 229, Limassol



Dubai

Unit 507, Level 5, Gate
District Precinct
Building 03, DIFC,
Dubai



Hong Kong

8 Queen's Road East,
Wan Chai, Hong Kong



Pakistan

322-G3 Main Blvd,
Johar Town, Lahore,
Pakistan



Singapore

68 Circular Road
#02-01, Singapore



United Kingdom

Office 408,
Coppergate House, 10
Whites Row, London
E1 7NF

shuftipro.com
sales@shuftipro.com