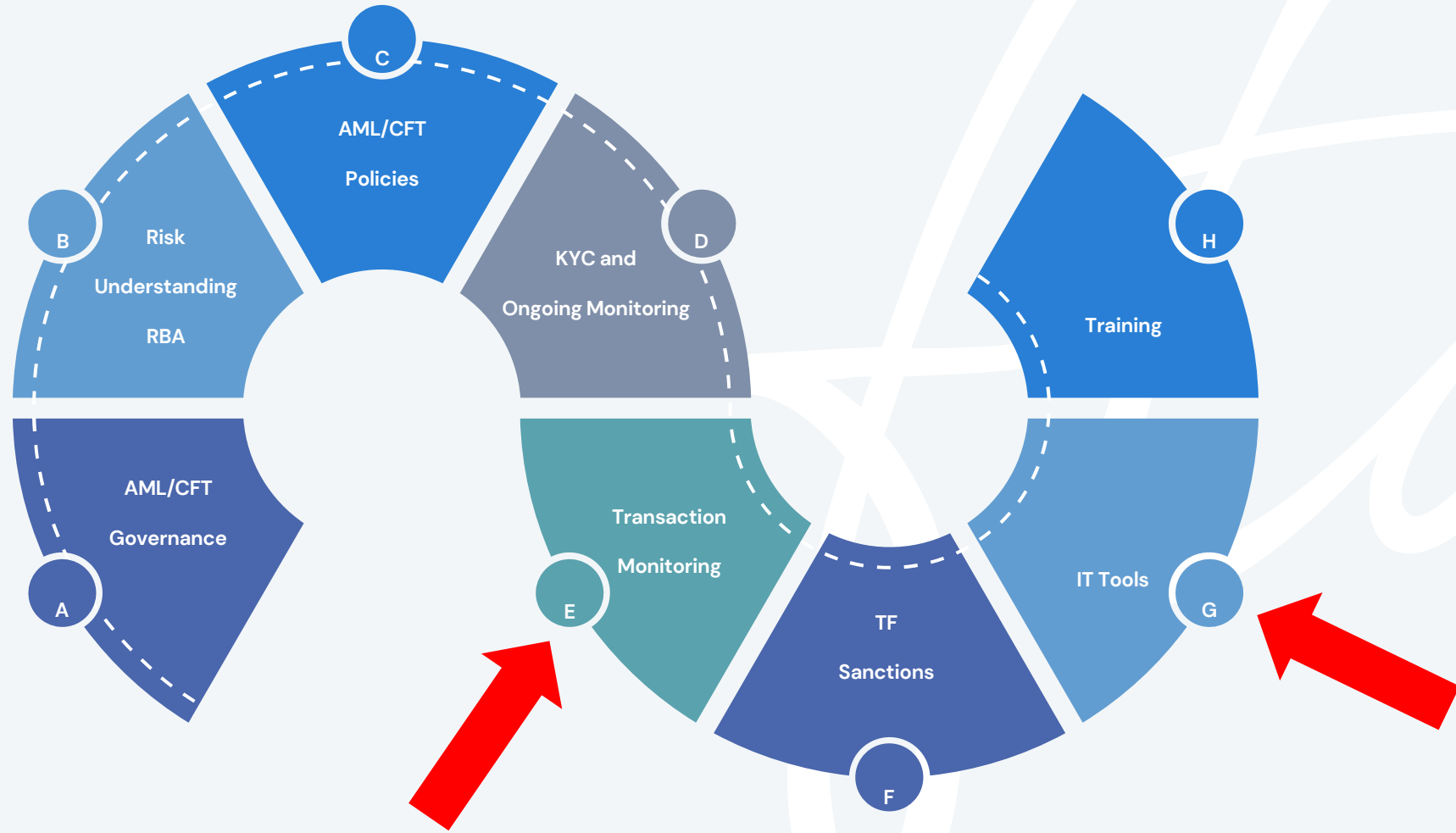


AML Tuesday's Session #25 on:

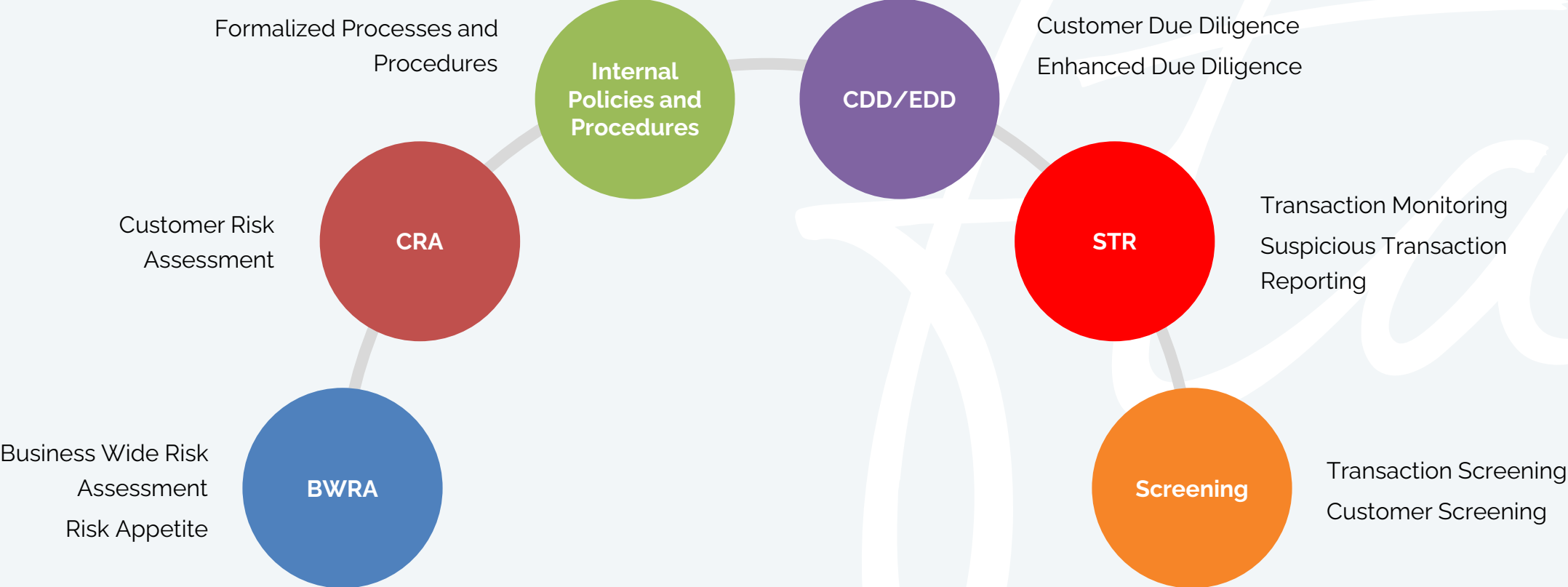
Transaction Monitoring, Tools, Scenarios, Best Practices

August 6, 2024

Key Blocks of AML/CFT Framework



Key Controls



FATF Risk Based Approach



"Ongoing monitoring involves checking transactions to ensure they align with the customer's profile and the nature of the business relationship."

Monitoring should be continuous or triggered by specific transactions. It could also compare a customer's activity with a peer group's.

Banks should adjust the extent and depth of monitoring according to their institutional risk assessment and individual customer risk profiles.

Example - Monitoring in high-risk situations: daily transaction monitoring, manual transaction monitoring, frequent analysis of information, considering the destination of funds, establishment of red flags based on typologies reports.

Key Aspects

Online/Real Time

- Blocking suspicious payments in real time
- Fraud

Offline

- Post event
- Negative Media/Sanctions

Periodic

- Historical Customer data to understand patterns and irregularities
- Data Aggregations weekly/monthly/Quarterly

Key Aspects



Risk Based



Thresholds, Triggers, Scenarios

Automated Alerts
Rule Based Algorithm
Case management



Customer Profiles

Integration with KYC



Reporting

Scenarios – Red Flag Indicators

Scenario

Typology

Red Flag

Scenarios – Red Flag Indicators

Fund transfer-specific red flags

Customer activities-based red flags

Customer-specific red flags

Scenarios – Examples

Unusual use of Currency

Use of multiple jurisdictions

Frequent changes to client data

Unusual use of debit cards

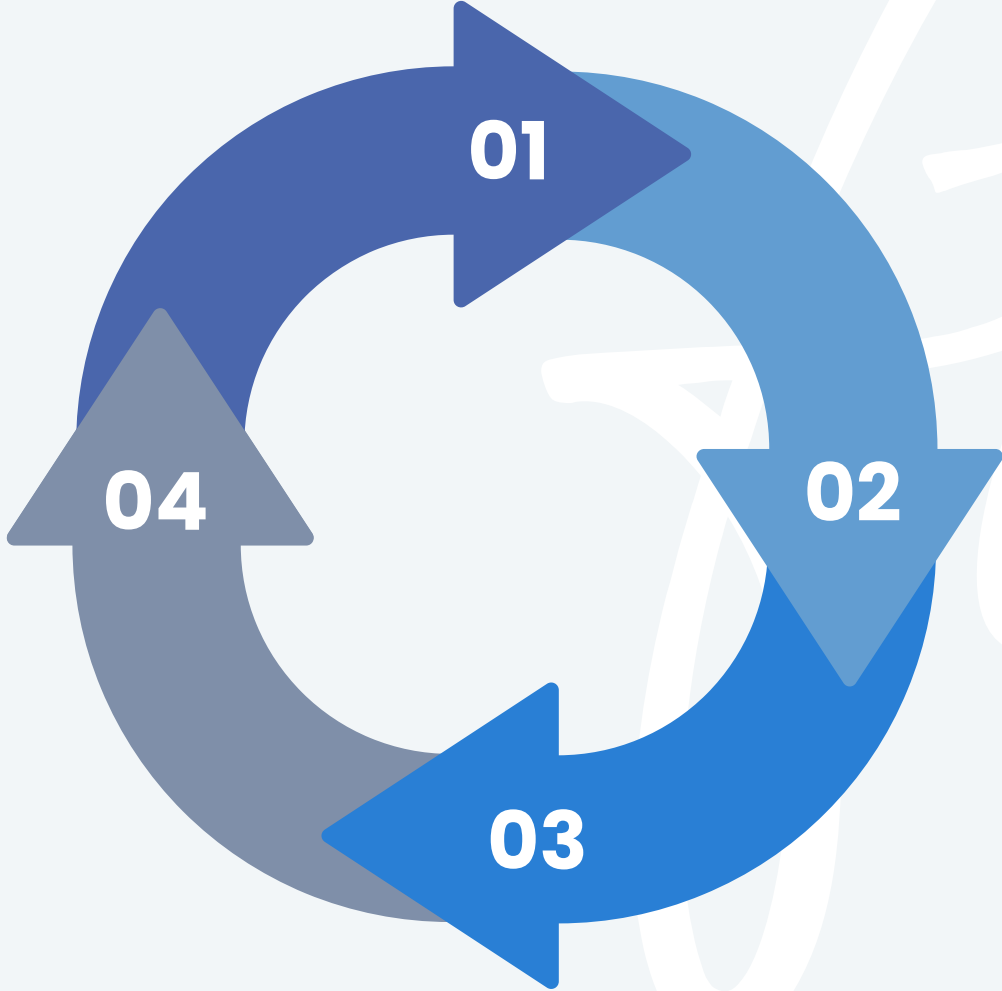
Excessive ATM activity

Dormant Account – Use of dormant accounts

Large-scale use of cash

Change behavior relative to peer customers

Transaction Monitoring



Process Flow

Internal Procedures defining process to identify ST

Implement Process

Implement Processes to review and manage alerts generated by the system, investigation and escalation

Assurance

Independent Review of Alerts
Algorithms
False Positives

Document Changes

Document any change within the system, thresholds, algorithms, scenarios etc

Process Flow – Example

Investigation involves collecting information from first line of defense

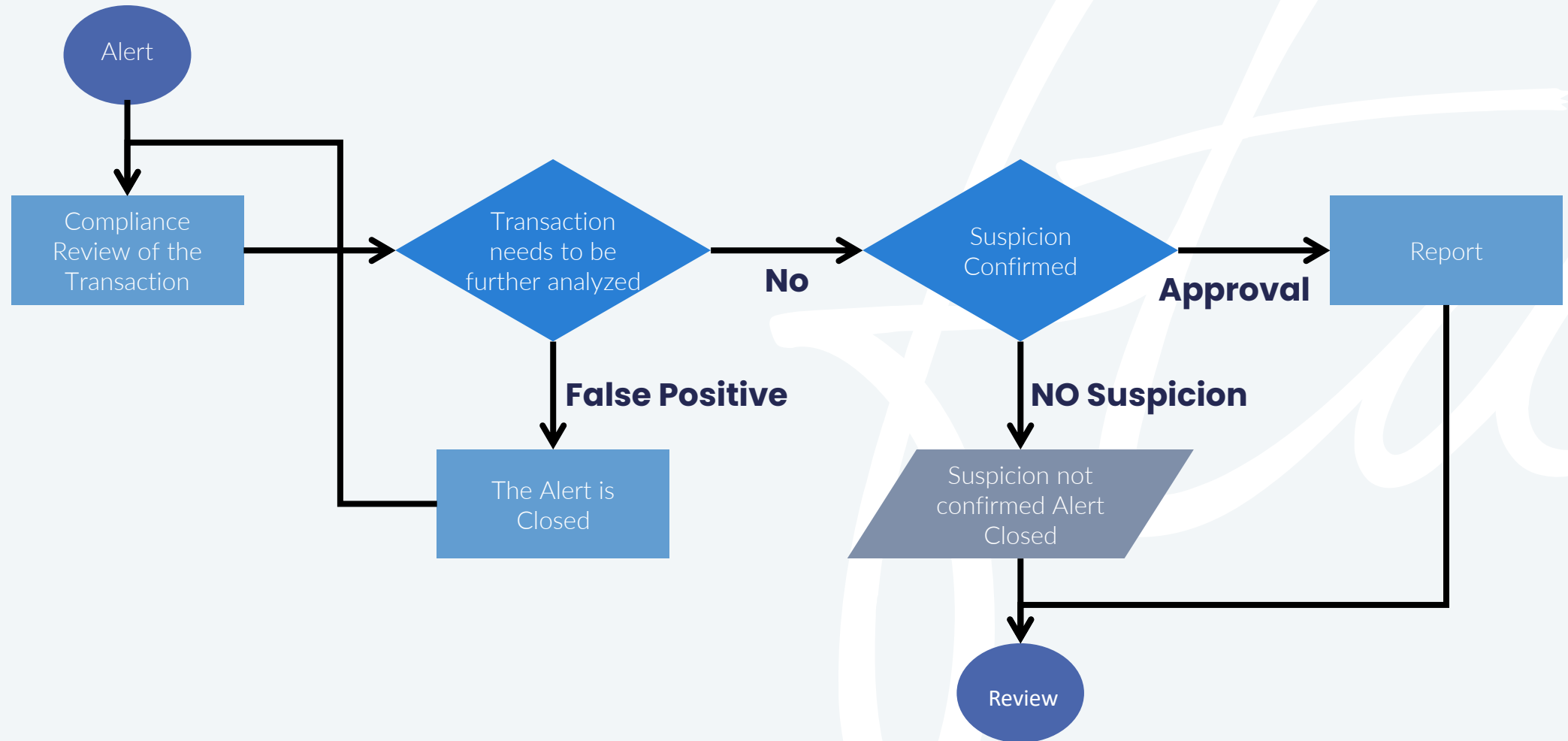
Suspicious cases are reviewed by more experience staff

Junior staff initially investigates alerts to gather information and filter false positives

Certain transactions are escalated to the head of the department/unit

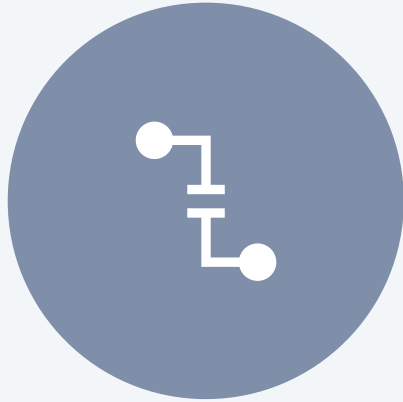
Certain transactions escalated to senior management

Process Flow - Example



Review of Closed Alerts - Sampling

Accuracy and Effectiveness



PROCESSES ARE IN PLACE TO MAKE CERTAIN NO DISRUPTIONS TO DOWNSTREAM AML/CTF PROCESSES OCCUR WHEN ANY CHANGES ARE MADE TO SYSTEMS



ALL SYSTEMS CHANGES THAT MAY POTENTIALLY AFFECT AML/CTF COMPLIANCE REQUIRE APPROVAL BY RELEVANT ACCOUNTABLE SENIOR MANAGEMENT



ALL ASSURANCE PROCESSES ARE IN PLACE AND AML/CTF PROCESSES ARE FULLY DOCUMENTED AND MAPPED.

Case Discussion

- FI “AZ” is financial institution conducting banking and asset management services
- FI “AZ” has approximately 20 000 customers
- “AZ” has conducted Business Risk Assessment
- Based on the BRA the risk associated with ML is Medium and TF low
- Total number of High-Risk customers based on the CRA is 2%
- Daily transactions screened under transaction monitoring system is around 200 P/D
- Alerts generated by the transaction monitoring system is approximately 100 P/D
- False positive ratio is approximately 25%

Big Picture



Periodic Analyses of funds flows



Flows to and from HR jurisdictions, verifying customer profiles and activity



Analyses of cash operations



Cash operations by residents from High-Risk Jurisdictions



Virtual Currency Transactions – identifying customers with high volume/number of operations



Online Platform Merchant Monitoring – Card Operations

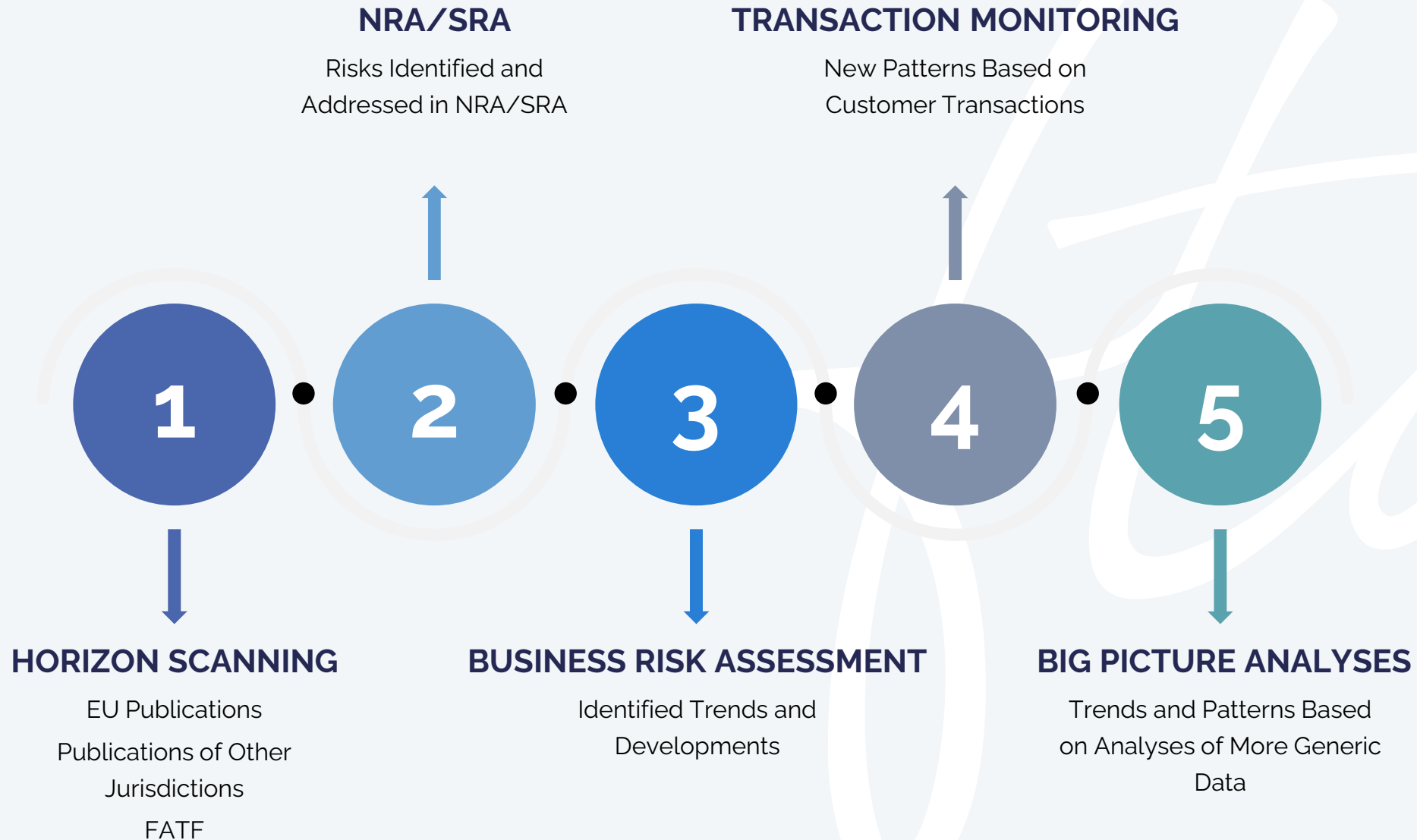


Analyses of customer base in Trade business (fund transfer jurisdictions, comparisons with previous periods)



Analysis of legal entities not operating in Monaco

Emerging Risks – Transaction Monitoring



Model Governance

Updated Regularly
to accurately
detect emerging
patterns

Testing algorithms

Scenario-based
Rules

Thresholds and
Anomaly Detection

Integration with
KYC tools

Documenting
changes – Audit
Trail

| Model Capabilities

Practical Dashboards

Big Picture Analyzes

Statistical information

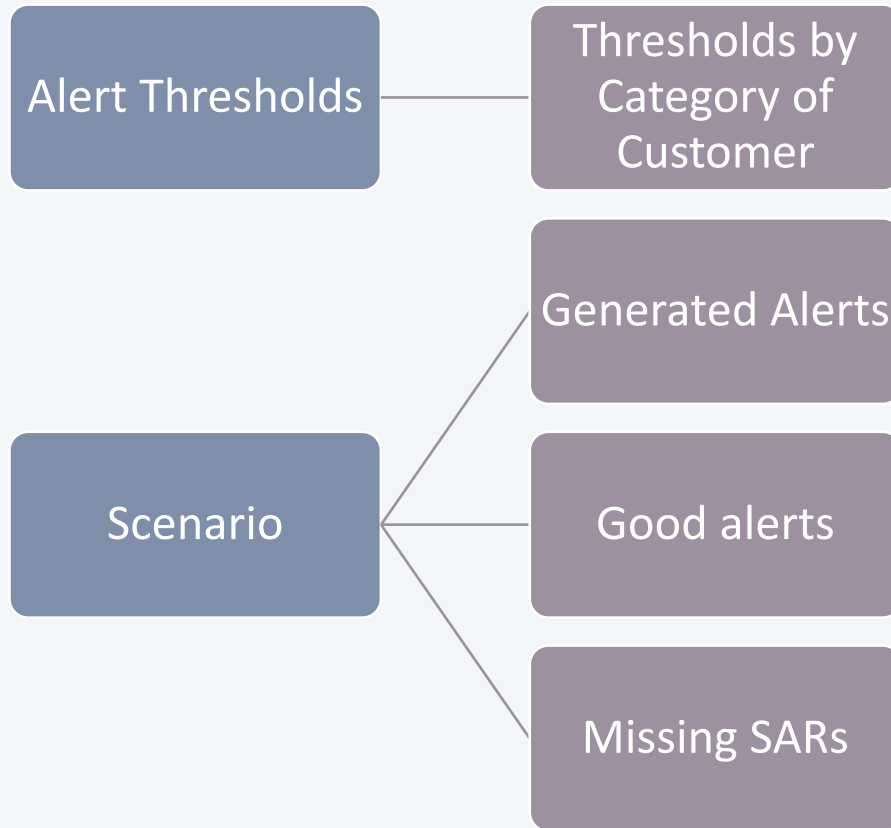
Alerts by Transaction Type

Customer Risk and Alerts

Open Cases

Time to Resolution

Model Validation



Data Validation

Scenario logic validation

Threshold values validation

Scenario Effectiveness

Common Deficiencies

Alert Backlogs

Making exceptions for specific customers

Alert investigation takes an unreasonable time

Transaction monitoring rules are not adequate

Scenarios and rules generate a high % of False Positives

Common Risks

Incorrect Segmentation Risk

Risks associated with Source Data and Inputs

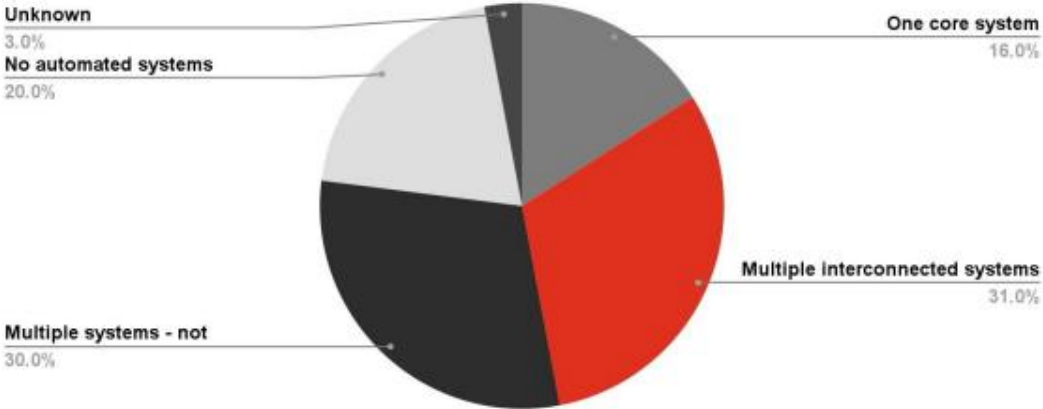
Incorrect configuration of the look-back period

Incorrect setting of the alert threshold or parameter

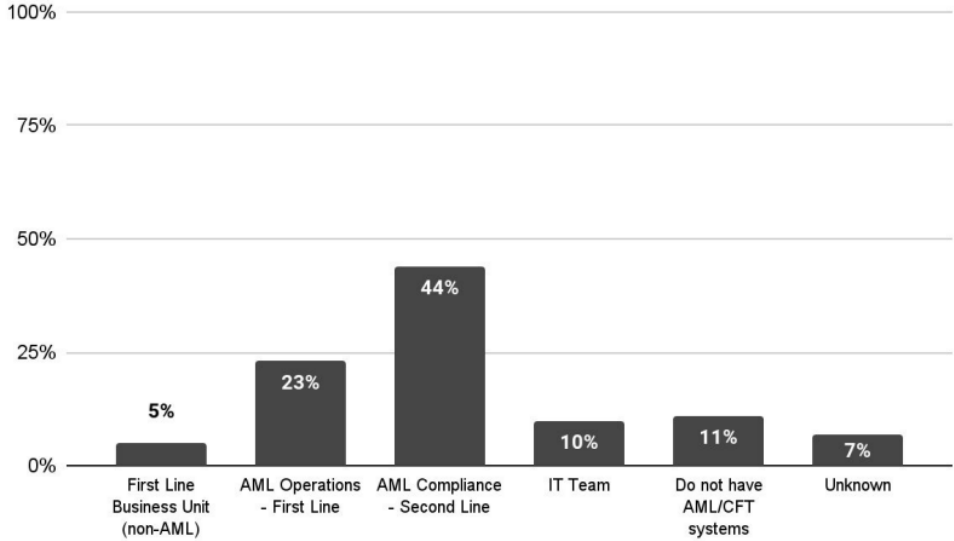
Common Challenges



Global Survey



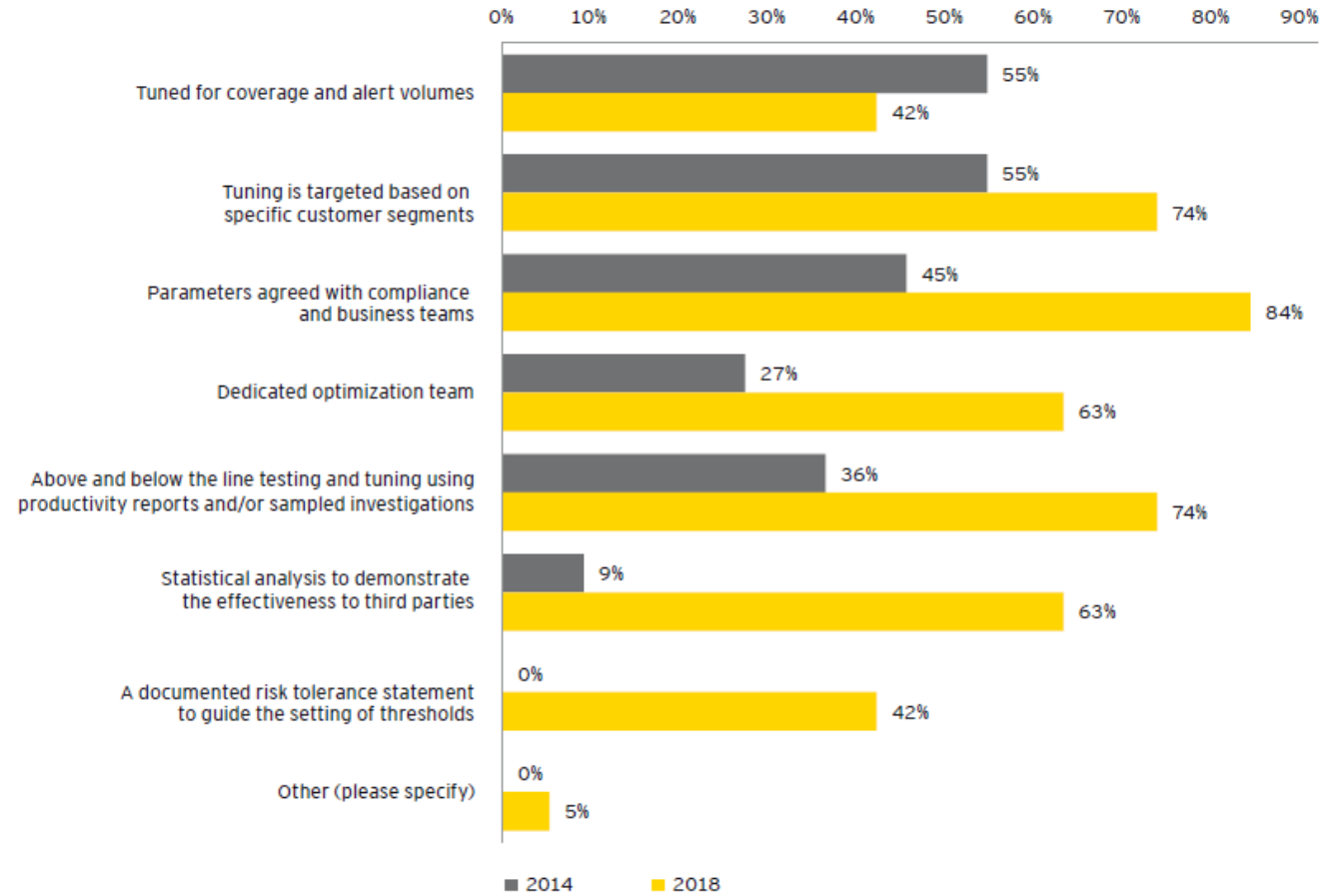
AML / CFT Tech infrastructure/systems



Ownership of AML/CFT Infrastructure

Source: PwC 2023 AML Survey

Figure 7 – What tools and techniques do you use to tune and optimize your TM scenarios?



Survey Results

Source: EY AML Transaction Monitoring EMEIA Survey Report 2018



*Thank you for your
time*

Financial Transparency Advisors GmbH
Zieglergasse 38/7/1070 Vienna, Austria

Phone: +43 1 890 8717 11

www.ft-advisors.com

<http://www.ft-advisors.com>

Next Session:
27, August 2024

Topic:
Sector-Specific
STR Typologies
and Red Flag
Scenarios Applied
in Practice

Today's Host and Presenter: Tamar Goderdzishvili