Deloitte.

Anti-Money Laundering Preparedness Survey Report 2020

Contents

Introduction

In the past decade, growth in South Asia has far exceeded that in other countries outside the region. Modernisation of the banking and financial services industry has been a major contributor to this growth. This resulted in significant credit availability for businesses and individuals, alongside better governance around managing operations.

However, with availability of formal credit, money laundering and terrorist financing activity has also increased in the region. Fraudsters and criminals have used banks and financial institutions (FIs) as conduits. The estimated amount of money laundered globally in one year is 2–5 percent of the global GDP, or in the range of US$800 billion to US$2 trillion. Though the margin between these figures is huge, even the lower estimate underlines the seriousness of the problem that governments, banks, and FIs need to address. In South Asia particularly, the rapid adoption of online payments and wallet technologies means banks and FIs have had to fast-track and enhance their know your customer (KYC), and transaction monitoring processes. The COVID-19 pandemic has further accelerated digital transaction volumes, changing customer behaviour. New emerging risks have compounded issues pertaining to Anti-Money Laundering (AML) compliance. As a result, efforts to combat money laundering need to be increased. As a result, the efforts to combat money laundering need to be increased.

With criminals using newer ways of laundering money and changing regulatory expectations, banks find it challenging to keep their AML compliance programmes effective, guarding against these increasing complex money laundering activities.

In this backdrop, we wanted to understand the preparedness levels of banks in South Asia to meet revised regulatory requirements and challenges faced by them in their AML compliance programmes. We undertook a survey of leading banks and FIs in India, Sri Lanka, and Bangladesh in January–March 2020. The survey covers the following areas – AML governance framework, customer due diligence, sanctions and trade-based money laundering, and transaction monitoring systems.

The findings outlines several key challenges faced by banks and our report outlines certain leading practices to support their compliance efforts.

We hope that the survey report will influence discussion and debate amongst banks, practitioners, regulators, and governments on how to improve AML and counter terrorist financing efforts.

KV Karthik
Partner – Forensic,
Financial Advisory
Deloitte India

Uday Bhansali
President – Financial
Advisory
Deloitte India

Executive summary/key observations

Strategic investments are required for AML compliance programmes

- About 81 percent respondents indicated that their AML programmes were compliant with regulatory requirements. Yet they felt that staying compliant to increased regulatory expectations in the future is a key challenge and listed the following top challenges – meeting increased regulatory expectations, enforcing current AML regulations, insufficient numbers of adequately trained staff, and increased pressure to comply with multi-jurisdictional directives. From an operational standpoint, reliance on manual processes, poor quality/inadequate data, and recruiting and retaining skilled staff were the top three challenges identified by respondents in managing an AML compliance programme. With increased regulatory scrutiny and expectations of *'If you could have known, you should have known'*, the onus remains on banks to adopt a proactive AML compliance approach.
- The risk-based approach ("RBA") is central to the effective implementation of an AML/CFT regime. One of the fundamental elements in implementing an RBA is Institutional Risk Assessment (IRA) that enables banks and FIs to understand how and to what extent they are vulnerable to ML/TF risks. Then, they should use IRA to ensure the judicious and efficient allocation of resources and create a robust AML and CFT compliance programme. Nearly 87 percent respondents indicated that an enterprise-wide approach to AML risk management appears to have been adopted. However, these efforts appeared to be largely siloed. The majority of the respondents indicated that they focus on key assessments, such as customer-risk assessment and geographic risk assessment capabilities, rather than an integrated business risk assessment. This can make it challenging to understand the complete risk scenario and pose questions on the effectiveness of the AML compliance programme.
- Regulators expect banks to have a consolidated view of customers and their transactions across businesses and jurisdictions, to identify unusual transactions and behaviour, or potential sanctions violations. Apart from investing a significant amount of money in systems and people, banks need to take a wider and long-term view (instead of trying to meet minimum regulatory requirements). The top three focus areas identified by respondents for better AML compliance in the future included the following: customer due diligence, control effectiveness and sustainability, and use of AI and bots to improve alert generation and reduce false positives.

Transaction monitoring and sanctions screening processes need a makeover

- Robust information technology (IT) systems have always been critical for an AML compliance programme. Although banks have increased their investments on automated systems for transaction monitoring and sanction screening over the years, these investments may have not borne fruit. Survey respondents identified key challenges in the areas of technology, process, and people. The problems range from technology-related issues (lack of data accuracy and sufficiency, and increased false positives), and process-related issues (limited coverage of known TM red flags) to people-related issues (dependencies on manual processes). Similarly, the issues related to the lower confidence level in screening solution (besides data accuracy and sufficiency, and false positives) include inadequate fuzzy logic capabilities and list management. Fines imposed recently on banks indicate that these issues are a part of ongoing struggle of banks, and question their efficacy of meeting AML compliance and regulatory expectations.
- Respondents also identified factors that affected their confidence in current screening solutions. These included data structure issues, poor integration with core banking systems, numerous false positives/negatives alerts, inadequacy of fuzzy logic capabilities, and limited automation to update regulatory and sanctions lists.

Customer due diligence continues to be a key focus area

- An effective KYC programme involves understanding customers' shareholding structure; identifying beneficial owners and senior management where applicable; collecting and verifying the requisite Customer Identification Programme (CIP) information; and storing and screening customer data. This information needs to be reviewed regularly as well as based on trigger events. Banks appear to be collecting the requisite information per requirements (as a part of the KYC process) and identifying beneficial owners at the on-boarding stage. However, the periodic updates of this information may depend on trigger events; about 72 percent respondents pointed to unusual activity in customer accounts as a source for the trigger. Further, only 63 percent respondents indicated undertaking adverse media searches regularly to update customer information and profile.
    - This can pose a challenge to the risk-based approach that faces issues due to changes in customer profile, product usage, etc. These challenges can subject a bank to significant client and counterparty risks. They have a direct bearing on banks' ability to become more "risk aware", apply accurate levels of controls and due diligence, and keep "bad actors" out of the bank.

Countering Trade-Based Money Laundering (TBML) continues to pose challenges

- TBML cases have been in the limelight because of various estimates putting it at billions of dollars annually; these "red flags" are amongst the hardest to detect. Banks have been facing difficulty in implementing and monitoring controls in their trade finance business to combat TBML. While controls can be put in place for documented trade, the greater issue lies in open account situations where banks and Financial Institutions (FIs) have far less visibility of an underlying transaction. TBML is difficult to spot because it is hidden amongst legitimate transactions or activity. It often involves genuine trade and the associated paperwork, with only the subtlest of clues hidden deep in the trade structure or trading histories that can indicate suspicious activities. These appear to be reflected in the survey responses, with respondents reported facing the following challenges: identifying any network of hidden relationships in data between trade partners and ports; estimating pricing and invoicing of goods (under invoicing and over invoicing); lack of a single automated system that can combine screening data; and determining if goods involved in the transaction have dual use.
    - Given that trade finance is a specialised area requiring understanding of complex documentation, products and pricing-related issues), 85 percent respondents indicated that their employers were undertaking specialised training for trade finance staff on AML risks. Additionally, about 46 percent respondents indicated undertaking quarterly risk assessments related to TBML, to evaluate the effectiveness of controls and identify improvement areas. Yet there seems to be a gap in mitigating TBML risks as about 86 percent respondents screened trade finance transactions against internal lists before permitting transactions.

Section 1

The evolving AML environment needs strategic investments

Rapid developments in financial information, technology, and communication have facilitated the movement of money anywhere in the world with speed and ease. This makes the task of combating money laundering more urgent than ever. Every year, US$800 billion to US$2 trillion is laundered. This is about 2−5 percent of the global GDP.[3]

To address this challenge, governments and regulators across the world have come up with legislation and guidelines that have evolved over the years. AML compliance for banks is no longer a standalone function but one that is increasingly complex. Its scope covers functions such as legal, risk, operations, and tax. With ignorance no longer being excused, minimum compliance with regulatory obligations is no longer enough.

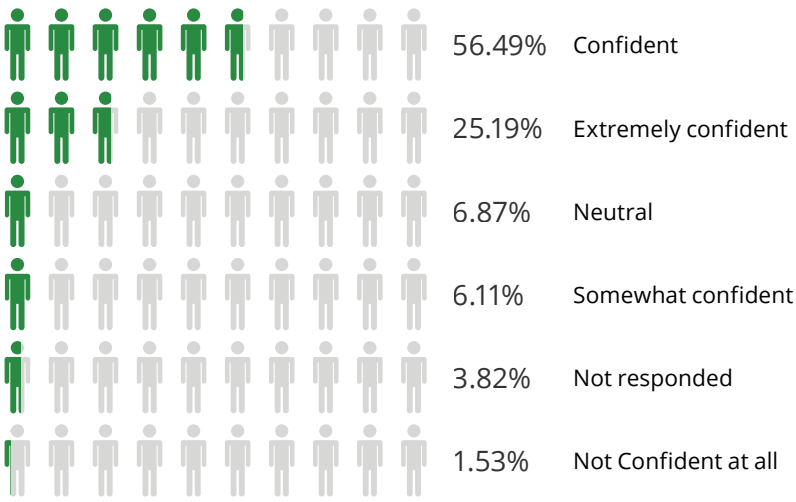
Banks face increased challenges in meeting heightened expectations

The focus on holding financial services firms accountable for deficiencies in their AML compliance programmes has been increasing across the globe, with heavy civil and criminal penalties for failure to comply. These penalties can be more pronounced for banks with a presence across various jurisdictions requiring them to comply with regulatory expectations in these countries and their home countries. As a result, AML compliance efforts may need to go beyond responding to incidents to a proactive and integrated approach to prevent compliance failure.

In the survey responses, banks have identified increased regulatory expectations and enforcement of current regulations and regulatory directives/ compliance with multi-jurisdictional requirements as key challenges. AML compliance management is also turning out be a battle for the best talent; often the first line of defence against money laundering is staff with specialised skills that can monitor transactions. The absence of such talent can pose challenges in AML compliance.

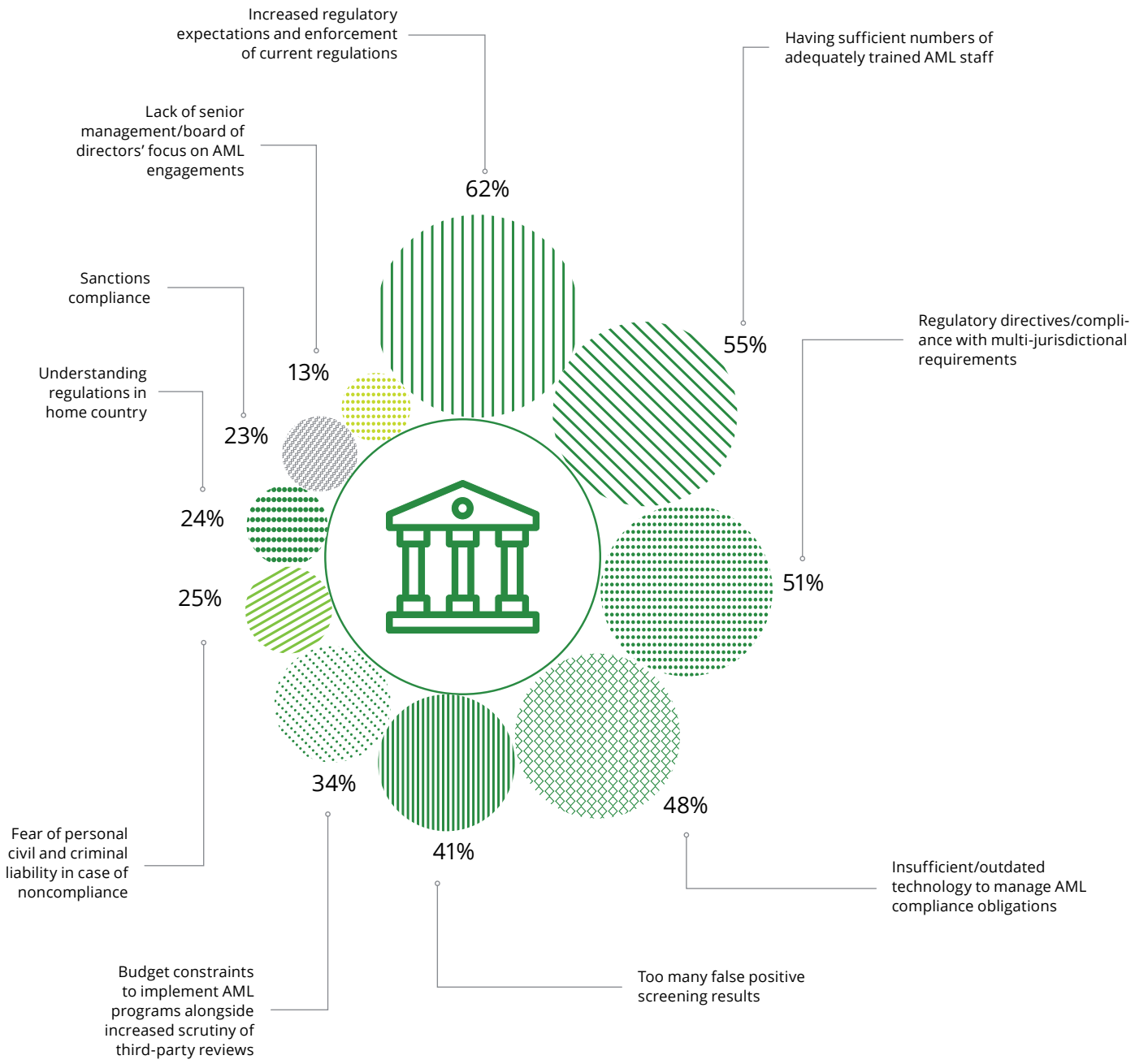
This is also reflected in the concerns expressed by the respondents. Historically, AML programmes have been incident driven with lean teams managing response to events or changes in regulatory developments. Taking an enterprise-wide approach enables organisations to increase the effectiveness of their prevention initiatives and streamline their financial crime-related activities. Breaking down silos and taking a cross-enterprise view of customers and transactions also make it harder for criminals to exploit gaps amongst business systems, databases, and countries.

How confident are you that your financial crimes prevention/framework is compliant with regulatory requirements and expectations?



[3] Source: https://www.unodc.org/unodc/en/money-laundering/globalization.html

According to you, what are the biggest AML compliance challenges faced by banks currently?
(This is a multiple choice question. Responses will not total to 100%)



Effectively managing change

Banks have always faced regulator-driven changes. The sheer volume of changes being introduced and their complex implementation and dynamic nature, differentiates the current environment. To manage these changes, banks and FIs should put in place a robust change management programme. This programme will ensure that they are aware of the changing regulatory requirements across locations where they have a presence. It will also ensure the effective implementation of these regulations and address the way they do business. Compliance is no longer an option.

Any regulatory change management should identify the applicable regulations, gather the necessary details, and ensure that work procedures and supporting information are provided to staff (who have the roles and responsibility to ensure compliance). Banks can consider the following approach for change management.

Mapping regulatory requirements

First, banks and FIs should understand their operations, including an assessment of products, services, and customers and the regulatory obligations that can apply. This will ensure that applicable regulations are identified and monitored for compliance. Banks can consider creating a regulatory catalogue containing details of regulatory bodies, elements of requirements, impact areas, sources, and supporting documents (as a ready reckoner) to facilitate change. Organisations may also consider including guiding principles from industry bodies, and leading practices as part of the mapping exercise.

Framework for managing regulatory change programme

Banks and FIs also face a challenge of the siloed approach and poor governance structure around managing regulatory change programmes. Banks and FIs should look at creating a centralised agile framework. The framework can constantly monitor any amendments to regulations, provide alerts at every change, and define the roles and responsibilities to ensure compliance. This requires a robust workflow process tool that helps deliver information to the responsible teams based on the impact of the requirements and avoid blind spots. Finally, putting in place an automated system is important. The system can easily integrate new/changes to regulations from identified data sources, and affected business segments.

Roles and responsibilities

A regulatory change programme requires interpreting guidelines to understand the areas of impact within an organisation in a consistent and structured manner. This requires identification of responsible persons within the organisation. These persons can take up the responsibility of assessing regulatory requirements, and mapping existing organisational policies and rules to ensure that compliance, policies and procedures are in line with regulatory directives.

Automation and workflow management

Banks and FIs should look at an integrated and automated solution to help identify the regulatory changes across jurisdictions on time to reduce cost and improve compliance obligations. For this, organisations should identify the best information sources (regulatory sites, content aggregators, industry bodies, etc.) and automate the feed to make any new guidelines/amendments to regulations available on a near real-time basis. Thereafter, this information can be integrated with a workflow tool that can process and route queries/potential actions to the right subject matter experts for review and analysis. Such a tool can also provide a dashboard to get a quick overview of changes, responsible parties, and status of activities/compliance.

Given the nature of the AML compliance regime globally and increasing regulatory directives across the world, change is inevitable. Adapting and implementing a robust change management programme can be an effective way to address changes while minimising non-compliance costs.

AML compliance is a board-level issue with continuing operational challenges and investments not bearing fruit

A bank's senior management is responsible for ensuring that its firm has effective AML policies, procedures, systems, and controls in place to manage risks in its business. Regulators across the globe have started increasingly focussing on the role of senior management in an AML compliance programme. As a result, the focus of compliance activities is shifting from responding to issues to a more proactive approach involving a prevention and detection mechanism. The senior management is expected to be involved in the following activities:

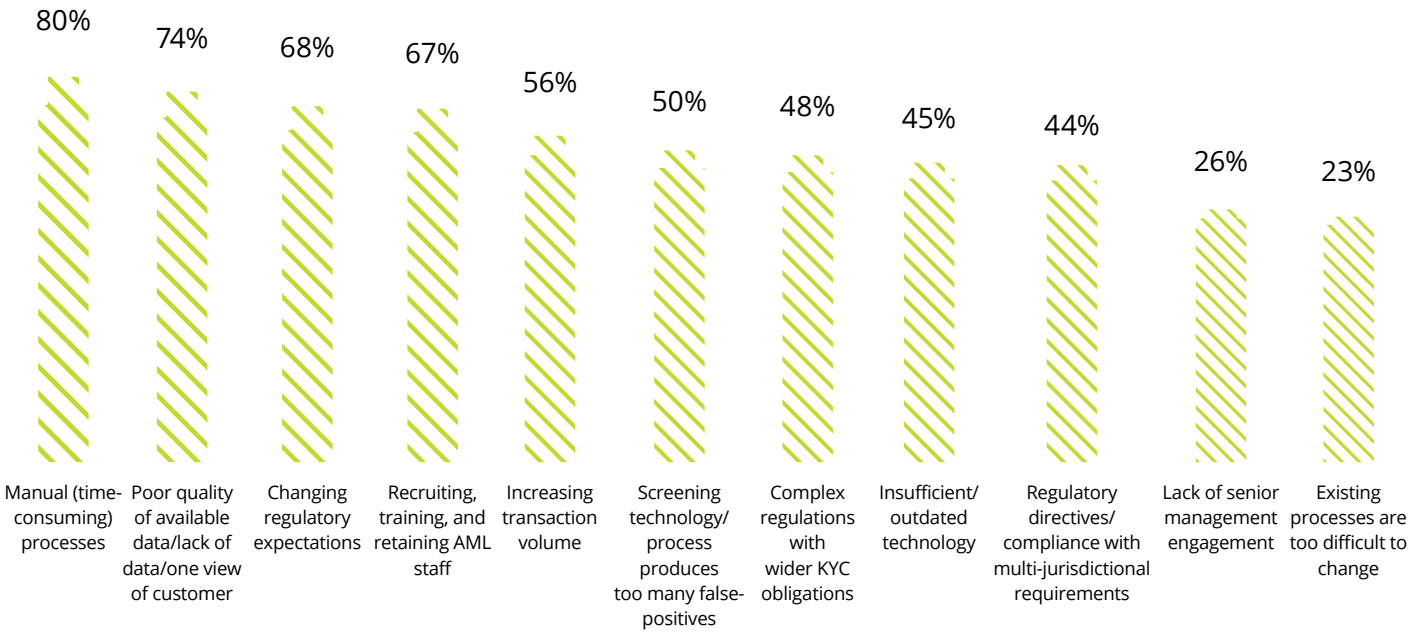
- Develop an AML risk appetite statement.
- Review and monitor IRA, and ensure they are in line with the risk tolerances set up by the bank.
- Allocate sufficient resources (both human and technological) to the AML compliance effort.

From an operational standpoint, banks have made significant investments over the years to update procedures, automate processes, and implement new systems to cater to the increased demand for regulatory compliance and business volumes. However, this appears to be still work-in-progress as respondents have indicated several operational challenges across technology, process, and people. In recent times, heightened regulatory scrutiny has pushed banks to seek a consolidated view of customers and their transactions across various services, products, and geographies. Over time, such high scrutiny levels are expected to become expectations.

In our view, due to a siloed approach and ad hoc investments, current systems at banks are characterised by dated IT systems and processes, resulting in the following issues:

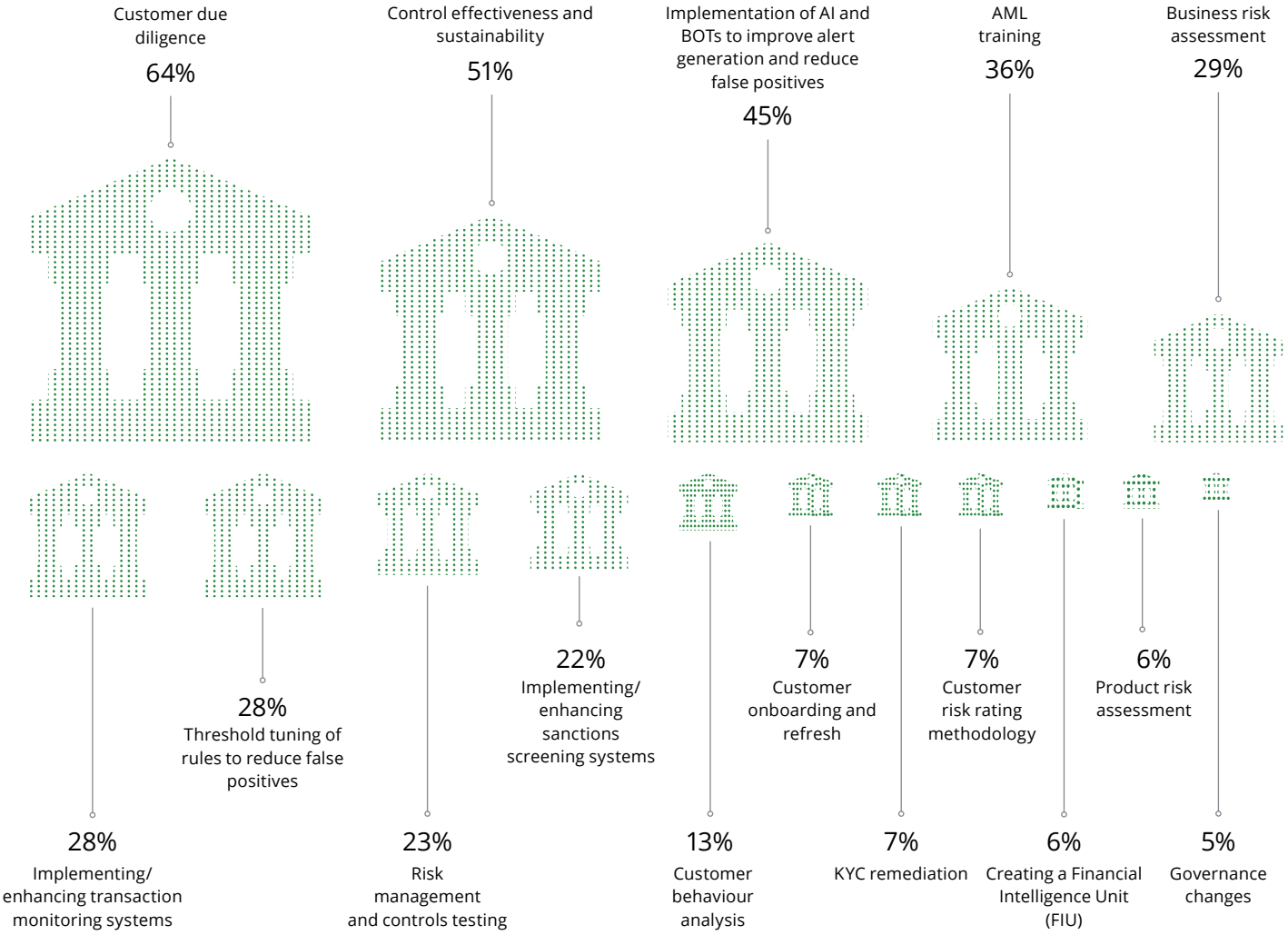
- Availability and quality of data
- Systems that are not integrated to meet the increased demand for compliance due to their inherent limitations, leading to significant manual processes in reconciling data

Please identify the top five operational challenges that your organisation face while complying with AML regulations (This is a multiple choice question. Responses will not total to 100%)



Therefore, respondents are looking at making significant investments in technology and tools to implement AI in transaction monitoring systems. This move will help reduce false positives, improve alert generation, and enhance control effectiveness. Investments appear to be focussed on customer due diligence or KYC, and transaction monitoring optimisation.

Where do you believe banks need to focus for better AML compliance in the next two years? Select the top three options that apply. (This is a multiple choice question. Responses will not total to 100%)

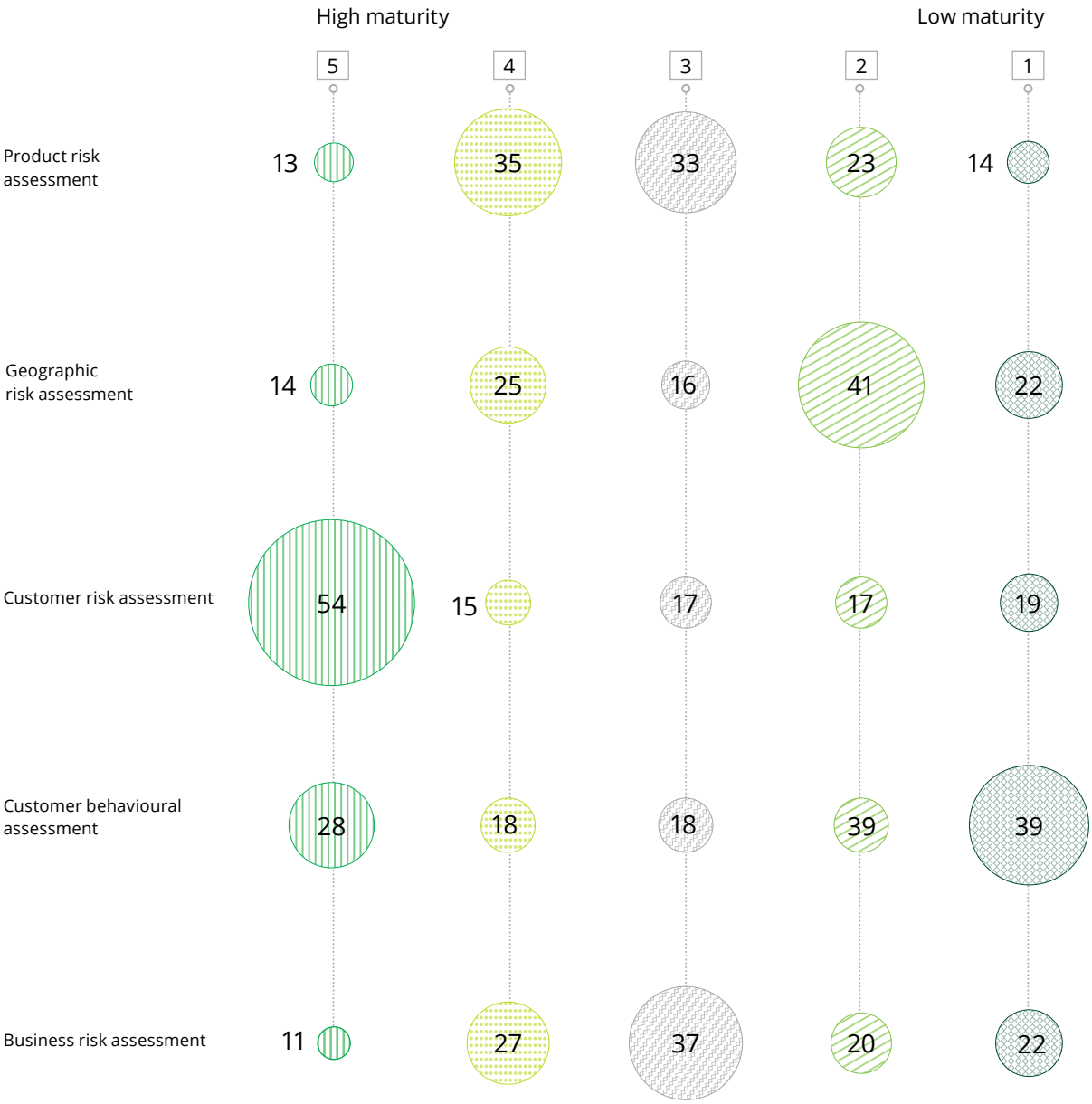


Banks are following a risk-based approach to AML compliance but more needs to be done

A risk-based approach to AML/CFT means that banks are expected to identify, assess, and understand the ML/TF risks to which they are exposed and take appropriate measures to the identified risks to mitigate them effectively. This ensures that the AML compliance programme is resilient and proactive (rather than meeting a minimum threshold), and not in tune with current risks that the organisation may be facing.

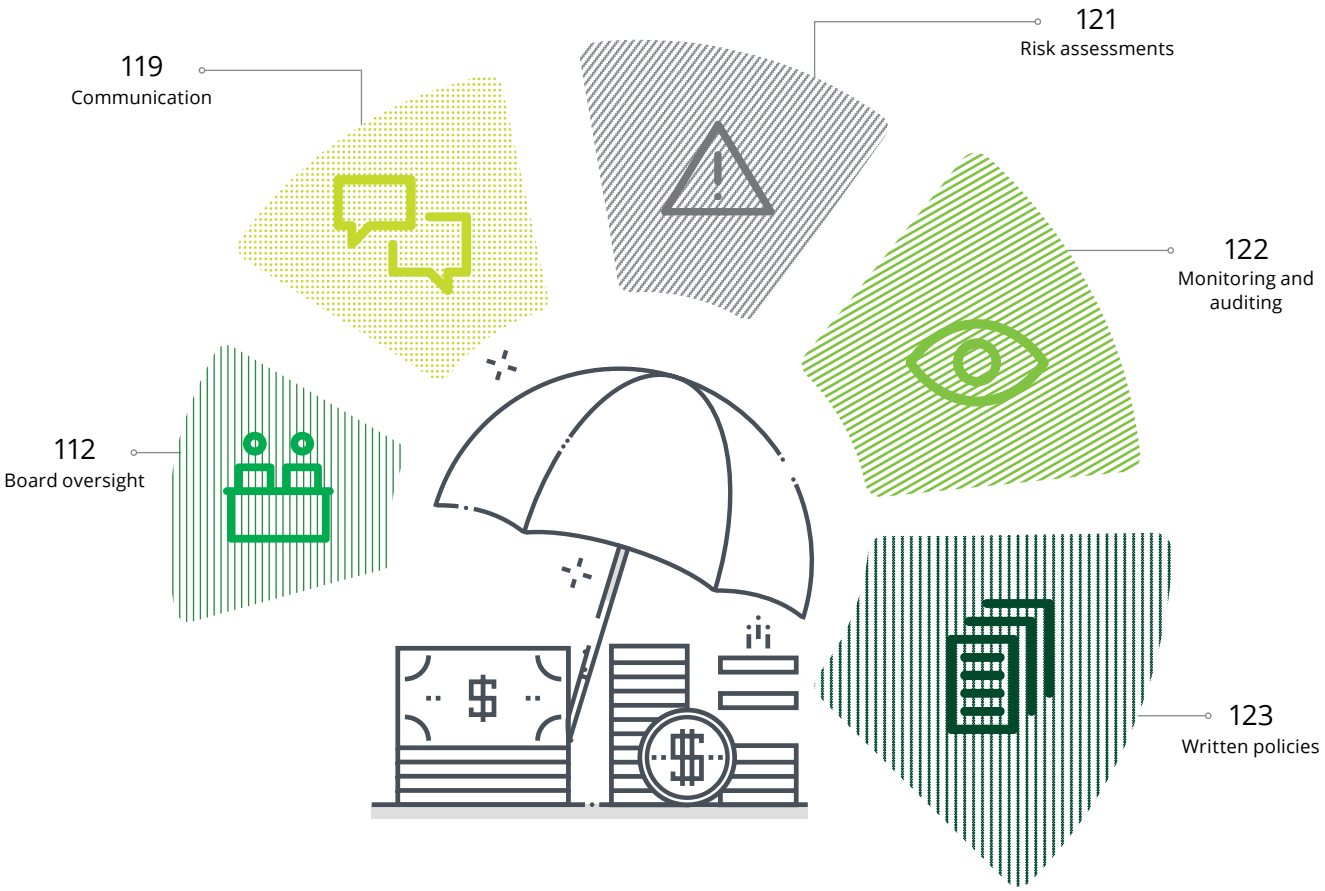
The majority of the respondents indicated that they undertake risk assessments as part of their AML compliance programmes. However, on dwelling deeper on the type of risk assessment undertaken by them, only 16 percent of respondents indicated that they undertook business risk assessment or IRA. A comprehensive IRA that identifies and considers the branch's products and services, customer types, and geographic locations (as appropriate), is key in determining inherent and residual risks. The output of this exercise will help banks prioritise resources to specific control functions and activities to mitigate AML risks.

Please rate the following components of the AML programme in terms of their maturity in your organisation. 1 = low maturity and 5 = high maturity



While quantifying costs of financial crimes (including direct losses, fines for non-compliance, and reputational damage) is difficult, this has become a significant issue for institutions. This is a board-level issue in the era of heightened regulatory scrutiny (given the impact that AML compliance can have on the reputation of a bank besides financial penalties). Banks are looking at AML compliance as a strategic priority (rather than a mere compliance requirement or a tick-in-the-box exercise).

Of the below list, please indicate which measures you have in place to manage AML compliance.
(This is a multiple choice question. Responses will not total to 100%)



Deloitte's IRA framework

A risk-based approach ("RBA") is central to the effective implementation of an AML/CFT regime. An IRA is a fundamental element of the RBA and the overarching requirement applicable to the relevant Financial Action Task Force (“FATF”) recommendations. It enables a bank or FI to understand how and to what extent it is vulnerable to money laundering/terrorist financing.

Various risk ratings/assessments are conducted as part of the AML compliance programme. These are sometimes misunderstood or interchanged for IRA and involve the following:

Country risk rating model

It is a mathematical model that rates countries by risk based on various independent sources. For example, membership in supranational bodies or presence in various lists.

Product and service risk rating model

It is a mathematical/judgmental model that rates product/service risk based on a list of factors. For example, products/services designated as a high risk by regulators and those possessing high risk attributes.

Customer risk rating model

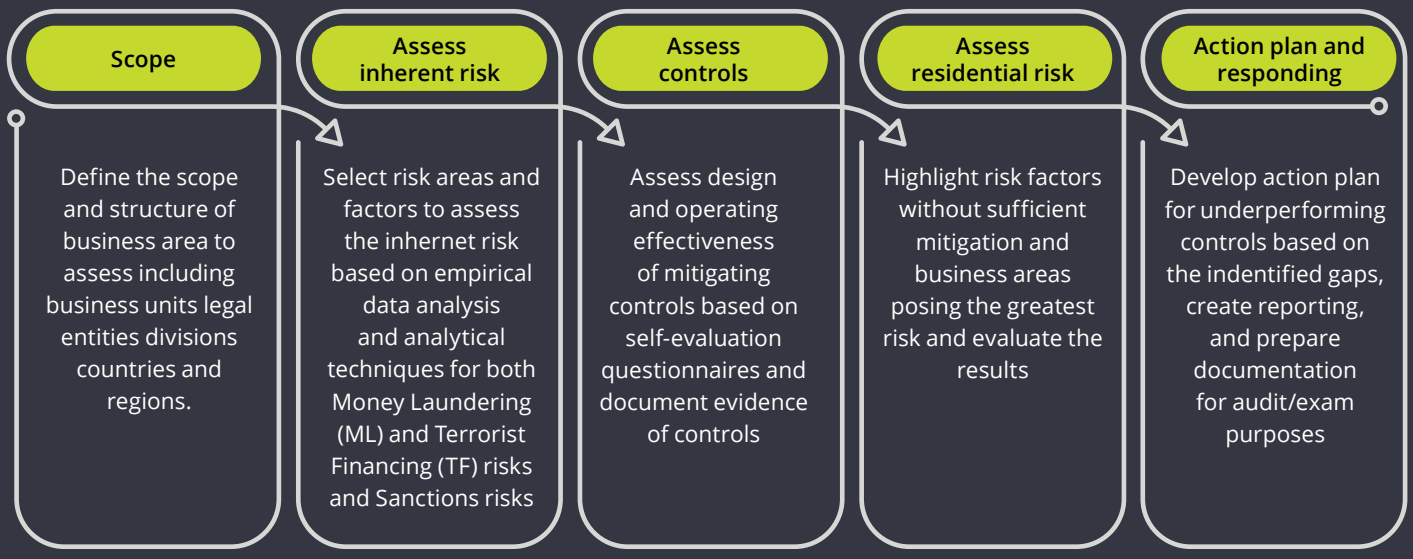
It is a mathematical model that rates customer risk based on a list of factors, including customer demographics, products/services/channels, geographies, and other risks.

An IRA is an anti-money laundering/counter-terrorist financing ("AML/CTF") risk assessment performed at the institutional level. The assessment enables the identification and assessment of general and specific money laundering/terrorist financing ("ML/TF") risks and mitigating controls in an entity’s AML/CTF programme. This will help establish the remaining residual risks and ascertain the AML exposure at the institutional level. The following are the key principles of an IRA:

- Align with the nature, complexity, and size of the activities being carried out.
- Document and communicate to relevant people within the financial institution.
- Review periodically and when circumstances change or relevant new threats emerge.
- Consider relevant inherent risk factors at the country, sectoral, group, entity, and business relationship levels. Perform the assessment in a holistic manner.
- Performed the assessment on the basis of a formally documented risk assessment methodology and approach. This approach must be applied consistently.

Conducting an IRA

IRA is a necessary but complex and resource-intensive assessment and its scale and scope should commensurate with the nature, size, and complexity of the organisation's business. An IRA is a three-step process that evaluates quantitative and qualitative risk factors relevant to the bank against mitigating controls to assess inherent and residual risk at the business unit and/or enterprise level. Some key considerations are listed below.



Scoping and methodology
The first step is to develop and use a standard methodology and format, and ensure that it is consistently followed across the organisation. Banks and FIs can use the guidance pronounced by regulatory authorities' and augment this guidance with industry leading practices. Documenting the methodology and results is also important to ensure that regulators and auditors can understand the process and how conclusions were drawn.

As part of the IRA, taking an enterprise-wide view of AML risks (covering subsidiaries, business lines, and functional units) and incorporating the assessment as part of the institution's overall risk assessment, are imperative.

Inherent risk assessment
Inherent risk is assessed across customers, geographies, products, services, and channels. The inherent risk should be calculated at the most granular level by identifying risk affected areas or factors using both qualitative and quantitative data and metrics. Risk factors are the underlying causes or circumstances where a bank/FI may become a conduit for money laundering. Inherent risk is determined by conducting an analysis of quantitative and qualitative data and metrics that comprise the impact and likelihood of each identified risk. One pitfall that should be avoided is mixing controls with the inherent risk assessment.

Controls assessment and residual risk
After the identification and assessment of inherent risks, evaluating controls to determine how effectively they offset the overall risks is important. These controls will include programmes and policy systems that are put in place to protect against the materialisation of ML risk and ensure compliance with existing regulations across the three lines of defence. Control effectiveness is assessed at two levels: 1) whether a control exists for the identified risks and 2) the operational effectiveness of controls.

After ascertaining both the inherent risk and the effectiveness of the internal control environment, the residual risk can be determined. This risk remains after applying controls to the inherent risk.

Alignment with national, legal, regulatory, and supervisory frameworks
An effective risk-based regime builds on and reflects a country's legal and regulatory approach, the nature, diversity, and maturity of its financial sector, and its risk profile. While identifying and assessing their ML risks, banks should consider national risk assessments and take account of any prescribed significant risk.

Non-alignment of IRA with the risk appetite statement
The senior management should approve the risk assessment, forming the basis for the development of policies and procedures to mitigate ML/TF risks. This reflects the risk appetite of the institution and states the risk level deemed as acceptable. Therefore, ensuring alignment in the IRA and the risk appetite statement issued by the bank is important.

Section 2

Customer due diligence continues to be a key focus area

KYC procedures are critical to assess customer risk and the first step in defending and managing money laundering risks. An effective KYC procedure involves understanding customers' shareholding structure, identifying beneficial owners and senior management (where applicable), collecting and verifying the requisite CIP information, and storing and screening the data per the customer's risk profile. This information needs to be reviewed regularly as well as on trigger events.

From an AML perspective, a KYC programme is designed to achieve the following objectives:

- Identify customers and verify their identity.
- Understand the customer profile and associated money laundering risks.
- Assign a risk rating to customers
- Conduct ongoing monitoring of customer risk and renew due diligence based on changes to information and activity that is different from what is expected.
- Make informed decisions about customers based on perceived risks.

Regulators expect banks to demonstrate that they understand their customer base and have considered the associated risks for their customers. An effective KYC programme must account for new money laundering threats and more advanced technologies. Given this dynamic, the regulatory pressure to create a more mature KYC programme is not expected to recede any time soon.

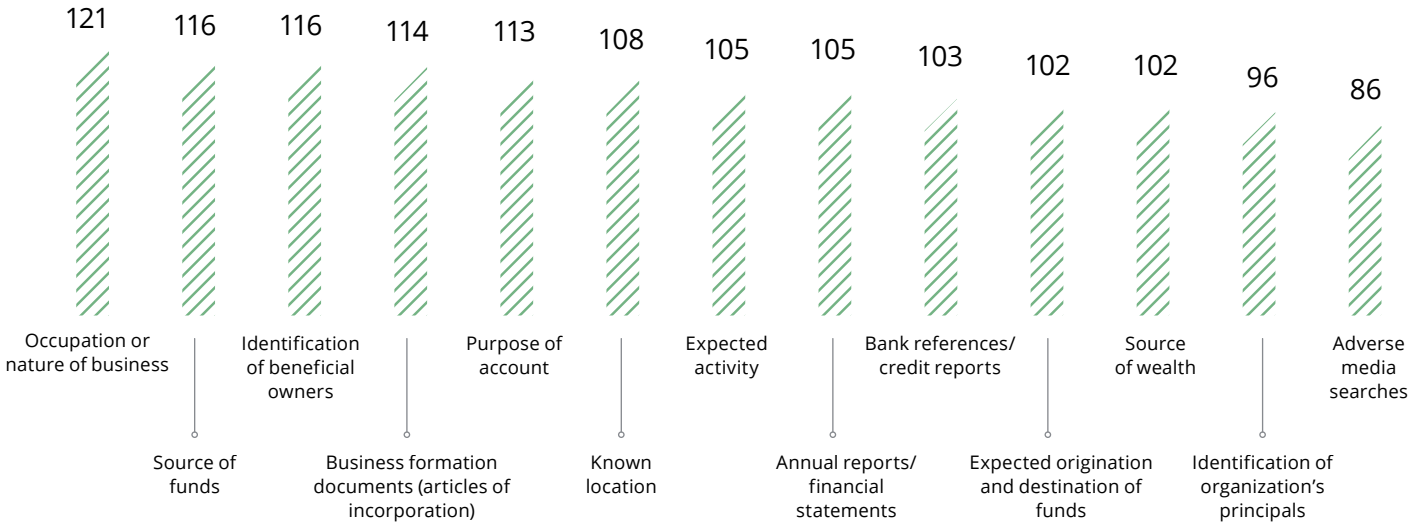
Customer due diligence continues to be the focus for banks

One of the key challenges identified by banks is the complex regulations with wider KYC obligations. With increased regulatory expectations and enforcement of current regulations compounded by regulatory directives/compliance with multi-jurisdictional requirements (as highlighted by the respondents), customer due diligence continues to be the focus with a majority of respondents putting CDD at the top of their agenda.

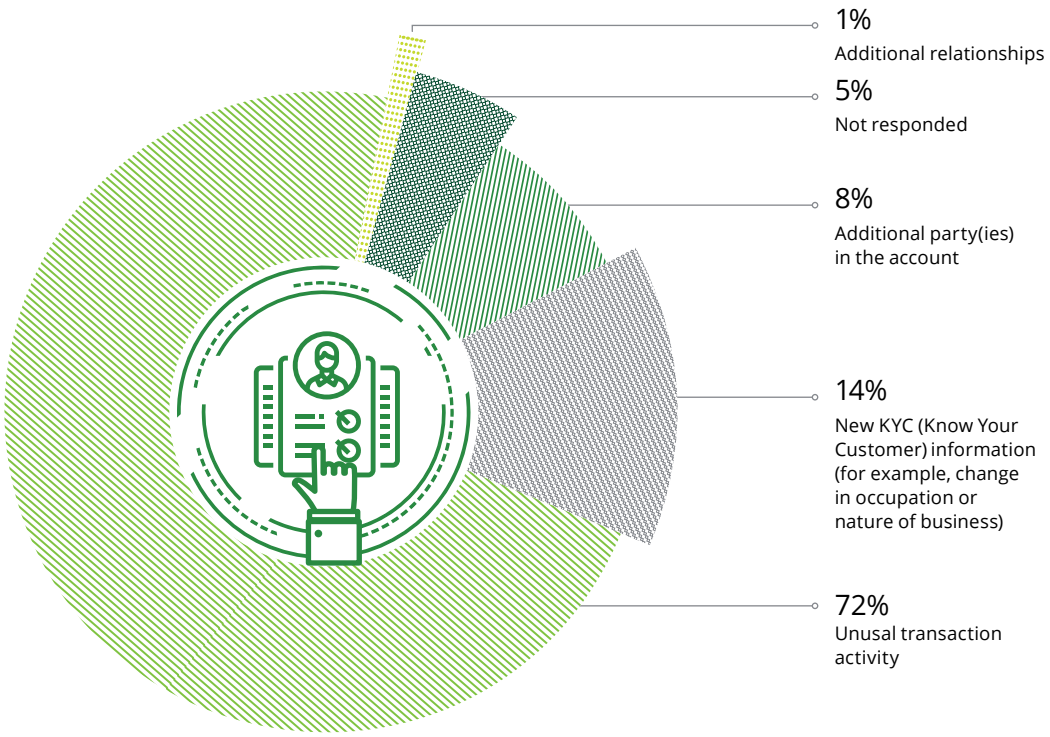
Where do you believe banks need to focus for better AML compliance in the next two years? Select the top three options.

It appears that banks are following the RBA approach and collecting information that will help them profile their customers at the on-boarding stage. However, it appears that the trigger to review or update the information/profile is undertaken by a majority of the respondents primarily when unusual activities are witnessed in the account.

Which of the following types of information does your organisation currently gather as part of its CDD process? Tick all that apply



In your view, what would trigger a review or update?

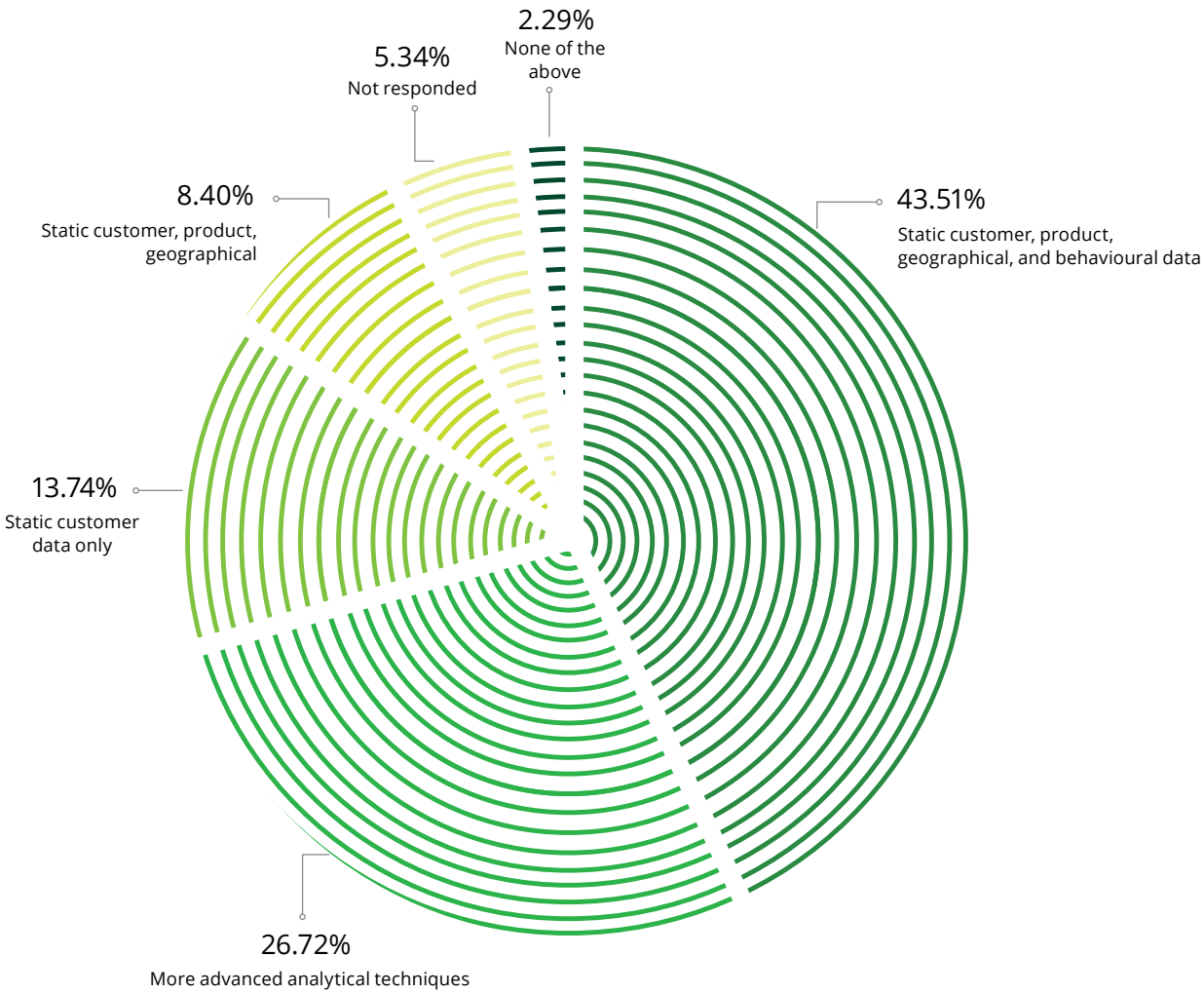


Customer risk rating is becoming more dynamic

Banks use customer risk-rating models as one of the primary tools under their AML compliance programmes. Traditionally, they deployed models based on static parameters, such as the customer types, industry, products availed, geographic location, Politically Exposed Persons (PEPs), and other risk factors. According to the survey, about 43 percent respondents still rely on this model. However, an effective customer risk rating model needs to be updated regularly. About 72 percent respondents said that they update customers' information primarily when they notice any unusual activity in the account, and not necessarily when changes to KYC information is available or new relationships/parties are added or identified. This poses questions on the effectiveness of the existing risk rating models used by banks.

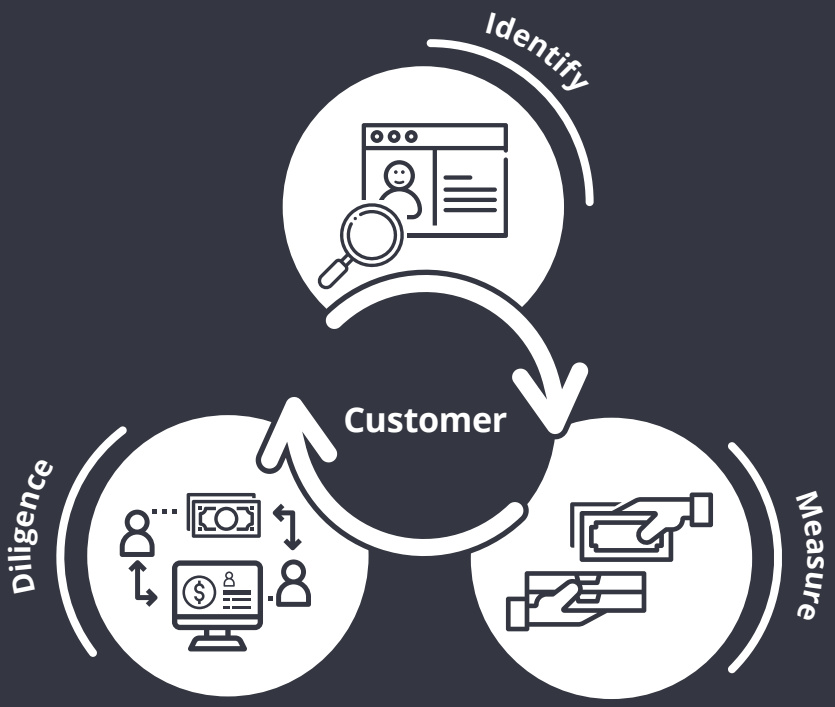
With changing regulatory expectations and technological advancements, banks across the globe have started looking at their customer risk rating models with a new perspective. They are looking at using data, including network analysis, transaction patterns, and link analysis, to dynamically reassess customer risk ratings. Using the wealth of information available from traditional and other sources, banks can develop advanced analytical models for dynamic customer rating.

What factors are incorporated in your customer risk rating algorithm?



Building a robust customer risk rating model

A robust AML customer information programme should be designed to achieve the following objectives:



- Identify and verify customers' identity.
- Understand customer profiles and associated money laundering risks.
- Assign a risk rating to customers.
- Conduct due diligence on customers based on the risk rating, undertake ongoing monitoring of customer risk, and renew due diligence where applicable.

In line with these expectations, a customer risk rating model is one of the basic building blocks for any AML compliance programme. At present, most institutions use a mathematical model that rates customer risk based on multiple factors, including customer demographics, products/services/channels, geographies, industries, and other risks (with weightage associated within each category to arrive at a customer risk score). However, a number of issues can lead to erroneous risk scores and misrepresent customer risks. The survey report points to some of these risks, including irregular updating customer information and inaccurate data that can lead to improper risk categorisation. For instance, with any change in customer behaviour, known associates, and transactional data, a different level of risk is posed to the bank. Should this data not be tracked and periodically updated, it can lead to high false positive rates. Banks may end up making significant efforts and incurring huge expenses towards resolution.

As a result, banks and FIs need to look at a risk rating/scoring model that is effective and dynamic (changes with variations in customer characteristics and transaction profiles). It should also consider changes in associated linkages with that customer (such as associates). This can include a combination of two or more of the following aspects:

1. Static risk factors

These attributes include existing information collected as part of the current model of customer risk rating at the time of on-boarding. This information includes customer business information, address/ location, jurisdictions, products and services availed, track records of customer relationship with the bank, and screening results (PEP, negative news, and sanction screening). The beneficial ownership and senior management for each entity can be also identified. The details of beneficial owners can be included as part of the rating process. Further, a process to regularly update this information must be institutionalised on the basis of trigger events and a tenure-based refresh of data.

2. Customer behaviour risk factors

These factors need to be considered as part of the ongoing monitoring exercise. This can include alerts generated for risky transactions (such as cash and non-cash structured transactions and transactions from/ to high-risk jurisdiction) that do not fit the profile of the customer and Suspicious Transaction Reports (STRs) filed, if any. Transaction analysis can also be used to identify potential changes to customer information (such as address and a change in business profile).

3. Network analysis

Network analysis can help identify hidden relationships based on internal (customer and transactional) and external data. For example, banks can look at existing customer base or external databases to identify linkages with other customers based on various customer attributes. This can be further extended to analysis of customer transactions wherein frequent transactions with particular customers or frequent 'wash transactions' might appear to be suspicious.

4. Statistical analysis

Banks can adopt various statistical and machine learning models to complement their existing customer risk rating methodology. A number of models, including the following, are available:

a. Network analysis to unearth patterns in data, identify complex and non-linear relationships, and update weights/coefficients based on this analysis

b. Clustering techniques to help discover natural groupings in data and remove redundant model inputs; these tools to assist in improving the accuracy of risk ratings and fixing data quality issues

c. Statistically identified outliers and peer group analysis to associate and compare profile of a particular customer with its peers from a similar segment

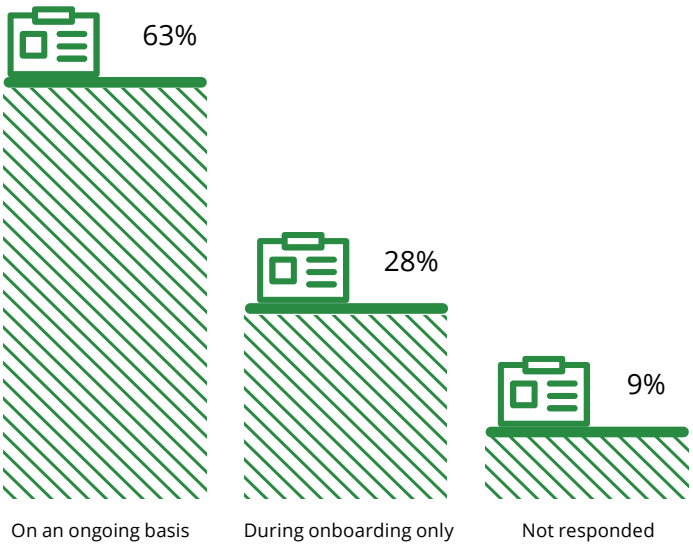
In a nutshell, data quality becomes an important and baseline requirement for any data-driven exercise. Using internally available information (which is periodically refreshed and reviewed) optimally; combining data science techniques and subject matter expertise; and continuously enriching models with incrementally available data customer points can help build a robust AML CIP programme.

Screening process needs to be more comprehensive

The main reason for customer screening is to assist banks in enhancing their customers' (or potential customers) risk picture and help identify if they are or could be linked to money laundering issues. These include information related to the following:

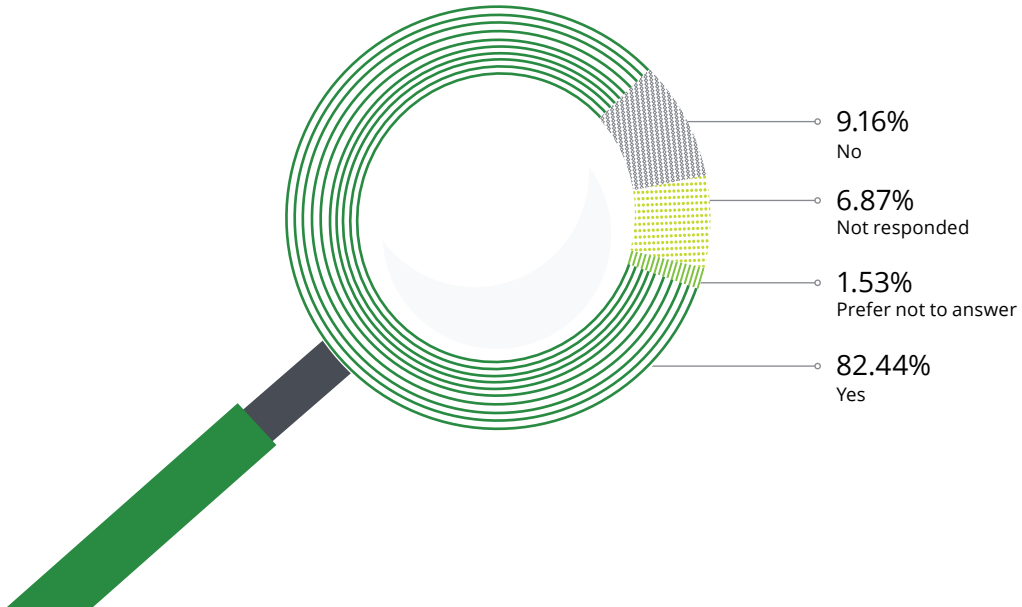
- Sanctioned entities or persons
- PEPs
- Have been suspected of committing financial crimes or convicted
- Negative news regarding people's background may affect risk profiles of customers/entities

When are adverse media searches performed?



More than 82 percent banks have indicated that they check for PEPs as part of the name screening process. However, only 63 percent respondents run regular adverse media searches. This is compounded by the fact that trigger events for review are undertaken primarily when unusual activity is noticed in the account; only about 23 percent respondents mentioned that their systems triggered a review request when additional parties or relationships were identified in the client data. This brings into question the effectiveness of the sanctions screening process that banks follow.

As part of the name screening process, do you also screen for politically exposed persons (PEPs)?



Section 3

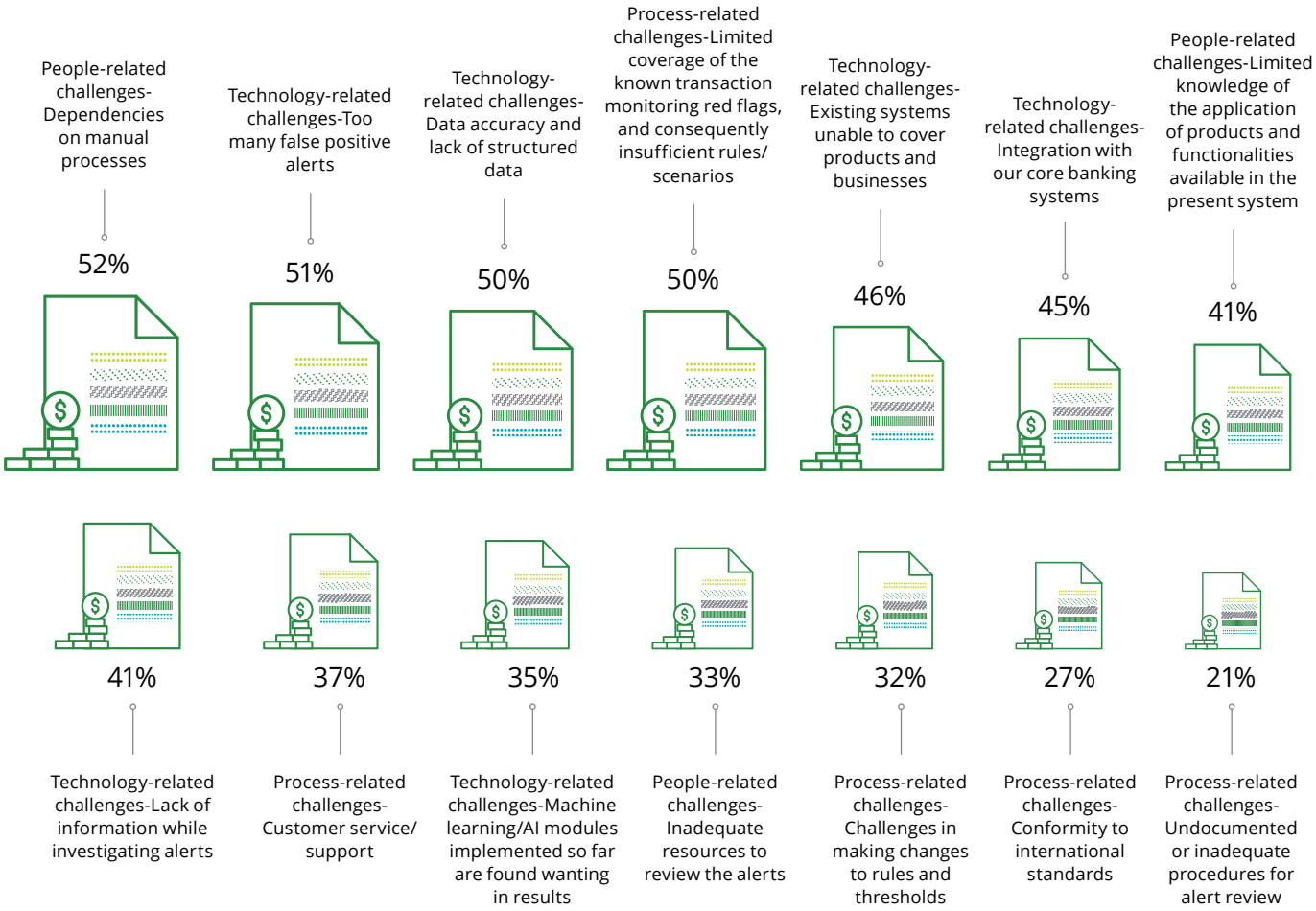
Transaction monitoring and sanctions screening processes need a re-design

More fraudsters and criminals are using new technologies, such as online banking, electronic payments, and cryptocurrencies, to move illicit funds across borders at a breakneck speed. This creates complex and layered transactions that are real-time, making it challenging to monitor and detect via traditional approaches. Therefore, banks have invested in robust IT systems for transaction monitoring and sanctions screening. However, the efficacy of these investments remains low (as a ratio of STR to alerts generated) for a variety of reasons.

Transaction monitoring systems need improvement

Detecting money laundering red flags using traditional transaction monitoring (TM) solutions can be inherently difficult because it involves complex transaction patterns/scenarios, quality/availability of data, ineffective interface with source systems, and substantial human involvement to clear the false positives generated by the TM system. These sentiments are reflected in our survey wherein, respondents have indicated issues across process, people, and technology.

What are the biggest challenges with your current transaction monitoring system? Identify the top five challenges across categories.



Although banks across the world have made significant investments in TM solutions, they continue to struggle with the effectiveness of these solutions. This resulted in a significantly low conversion ratio (STR/ alert generated). One of the key reasons could be the reliance on outdated rule-based transaction monitoring systems. These systems work by screening customer activity against a set of rules and outliers are flagged for investigation by the compliance team. This increases the cost of compliance (because of a large percentage of false positives), and presents constraints in terms of it not being agile enough to monitor new and specific typologies of money laundering.

In our view, some of the key issues in the current TM framework can be attributed to various factors ranging from systemic constraints, integrations of TM systems, and implementation issues including but not limited to:

One size fits all approach:

Many existing TM systems are either developed and implemented in-house or rule-based legacy systems. Although these systems are simple to implement and understand, they are inflexible as they rely on parametrised thresholds to identify "red flags". At the transactional level, this does not help banks to meet their objectives of a single view of customers. To overcome this issue, banks use the workflow tool to aggregate alerts for customers as a workaround to review all alerts of customers together. Moreover, given the inflexibility of the systems and changes in the internal and external business environment, banks have created a number of new rules/ scenarios to identify suspicious transactions. The number of scenarios has increased significantly over time and created overlaps between rules/scenarios, leading to duplication of efforts. These factors lead to significant false positives with many banks having a conversion ratio of less than 1 percent.

Further, relying on implementing an off-the-shelf product with standard scenarios is easy for banks. However, regulatory bodies expect TM systems to adopt a risk-based approach customised to the risks that banks face based on their institutional risk assessment.

Lack of data

The effectiveness of any AML transaction monitoring tool depends on data quality. Bank systems have evolved over the years. Many of them were originally designed to collect and process data for various business purposes that may not be specific to compliance requirements. As a result, these systems are siloed and data quality is often questionable, making them "unfit for purpose".

Banks need to understand their data sources from where information is fed into the AML transaction monitoring systems. The lack of standardisation in the way data is obtained, stored, or made available from each source is one of the biggest challenges that banks face. The second issue is multiple sources of data used by banks. As data is rarely consumed at the point of origination and flows through multiple systems/processes before it gets used, it could get modified or may not be comprehensive. Banks need to fully understand the source of the data being fed into their transaction monitoring solutions to ensure that it is suitable for the scenarios in the TM system.

With an increased focus on transaction monitoring compliance by regulators, banks are expected to put in place a robust data quality programme. The programme will help banks identify data sources containing relevant and accurate information, and ensure the data flows through to the transaction monitoring.

Increased manual intervention

Significant increase in volumes, increased false positives and a low conversion ratio, together with inefficient alert review systems and process, can add to open alerts and backlogs.

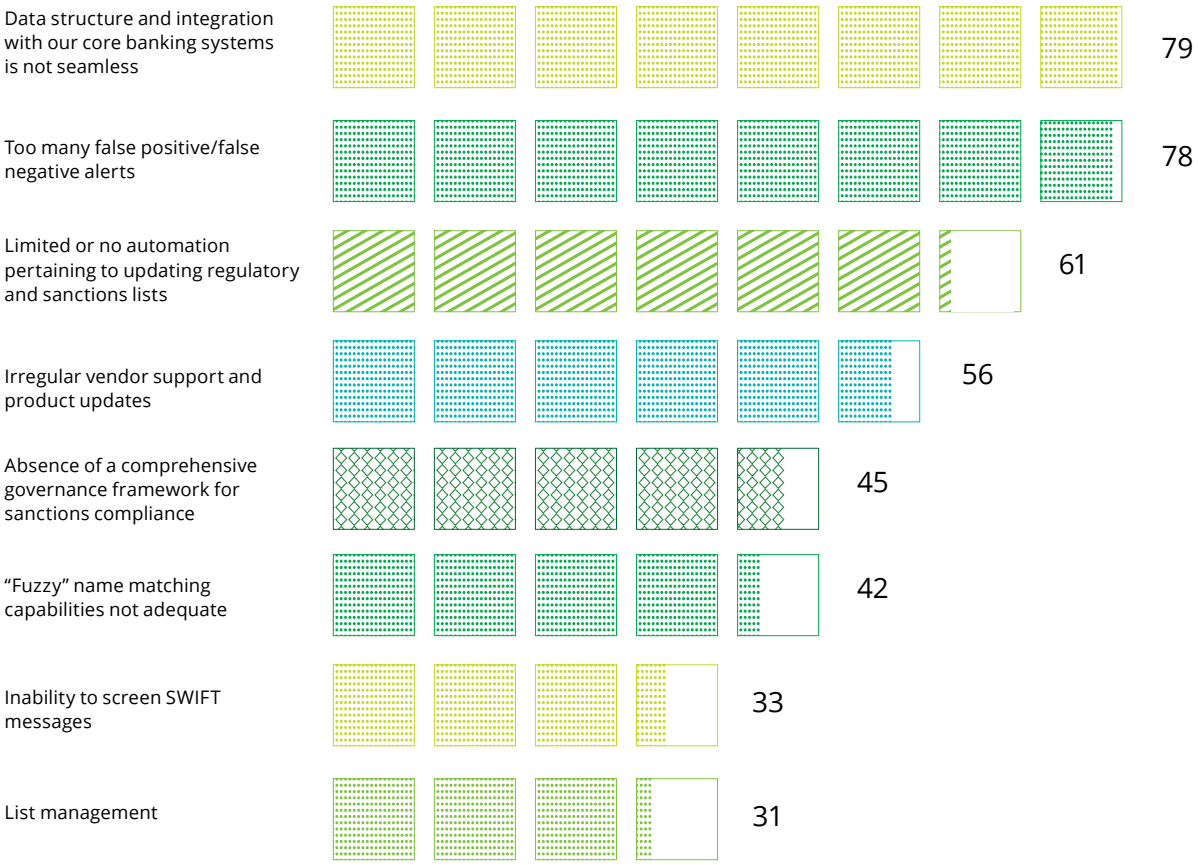
The least focused area in any TM system is the alert handling process. The TM team reviews system-generated alerts based on rules/scenarios to determine if they are suspicious or not. This, coupled with lack of visualisation options and one view of customer alerts, leaves the alert disposition team with limited ability to understand underlying data and alerts generated. These factors also make it difficult for the team to undertake a comprehensive review and determine suspicious activity.

Screening solutions remain a sore spot

Regulators across the world have increased their focus on watch list screening programmes. This is reflected in the significant fines that have been imposed on banks. The increased focus has turned the spotlight on the screening technology and the associated process. An effective screening requires accurate data preparation; sophisticated matching; and comprehensive investigation, auditing, and reporting processes.

Nearly 60 percent respondents indicated that they were struggling with a significant number of false positives and growing complexity of the task (as banks need to check a wide variety of available information against an ever-longer list of sanctioned individuals and organisations). Further, 22 percent respondents said complying with the list management/updating process was a challenge.

What are the factors affecting your confidence in your current screening solution? Tick all that apply.
(This is a multiple choice question. Responses will not add to 100%)



IT investments are essential for the intensive screening involved in sanctions compliance. However, the difficulties inherent in the task and the still-developing software pose some key challenges to global institutions.

Ever-increasing list of sanctions published by multiple agencies/ government bodies: This, coupled with the increasing expectations of sanctions compliance programme, makes it more difficult for banks to effectively identify and manage sanctions risk. The first and basic task for any bank's compliance programme is to identify the list against which they need to monitor their customers and transactions. Given the nature of these lists and the global nature of their operations, banks must identify specific lists that need to be catered to. Any unnecessary addition to the list will lead to increased alerts. Any significant deficiency in these lists will result in non-compliance and possible blocking of transactions by their correspondent banks or lead to non-compliance.

Dynamic lists. Banks are required to screen data against updated lists. This, coupled with the dynamic nature of customer data, requires banks to undertake periodic screening of their existing customers against the updated lists to ensure that they are compliant. Some of the existing systems provide for automatic updating of the lists. In other scenarios, banks manually update lists in their systems based on certain triggers notifying them of any changes/updates to lists. Therefore, list management is an important element of sanctions framework to ensure that banks can demonstrate their compliance to regulators.

The inconsistent method of transliteration of names is another issue where partial names, aliases, transliteration, different spellings of names, name reversal, shortened names, etc., are common. The degree of fuzzy logic threshold definition may lead to either increased false positives or missing the name altogether. This leads to a situation where banks are put in a quandary to decide on increased cost of investigating false positives or non-compliance to regulatory requirements.

FIs must use IT solutions to deal with an increase in transaction volume. However, unfortunately, just implementing an IT solution does not solve this problem. This can introduce a host of other difficulties. The biggest issue for a software solution is the inherent difficulty of the screening process, i.e., calibrating the fuzzy logic programme and integrating data that may reside in silos. An effective solution needs to cater to multiple lists with varying degrees of data quality, and incorporate fuzzy logic to cater to these variations.

One of the prerequisites of an effective sanction screening process is data quality and sufficiency. With siloed systems, banks need to invest in substantial manual processes to meet this requirement. The other expectation is that banks use clean data for compliance purposes. This requires them to identify data sources and validate the integrity, accuracy, and quality of data to ensure that accurate and complete data flows through the transaction monitoring and filtering system. Putting in place and demonstrating a robust data quality programme (as part of their sanctions compliance programme) is an essential requirement for banks.

A robust sanctions compliance programme would include the following aspects:[4]

Robust sanctions policy:
It can cover the relevant regulatory requirements, including the lists to be covered and the elements to be screened as part of the sanctions screening programme. This should take into consideration jurisdictions where banks are located and they conduct business, location of banks' customers, the products and services they offers, and their sanction risks.

Integration with high-quality and a wide range of trusted data sources:
Banks need to consider how they manage their lists to include sanctions lists from relevant bodies and the data to be screened (that include customer and transactions elements). Banks should ensure that data is consistent and adequate, and interfaces with various appropriate source systems.

Documenting the screening process and system:
Banks need to design systems that minimise their exposure to sanctions risks; document their decisions and rationale; monitor their implementation; run them rigorously; and review the changing risks regularly. Implementing screening control processes requires an understanding of various methodologies and technologies available. There are a number of screening systems with fuzzy logic as a feature to reduce false positives. Banks should ensure that the technology for matching names and accounts are calibrated and tested to ensure no true match with lists is missed and documented to show how they are configured demonstrate how it fits the purpose of detecting and manage the specific sanctions risks to which they are exposed.

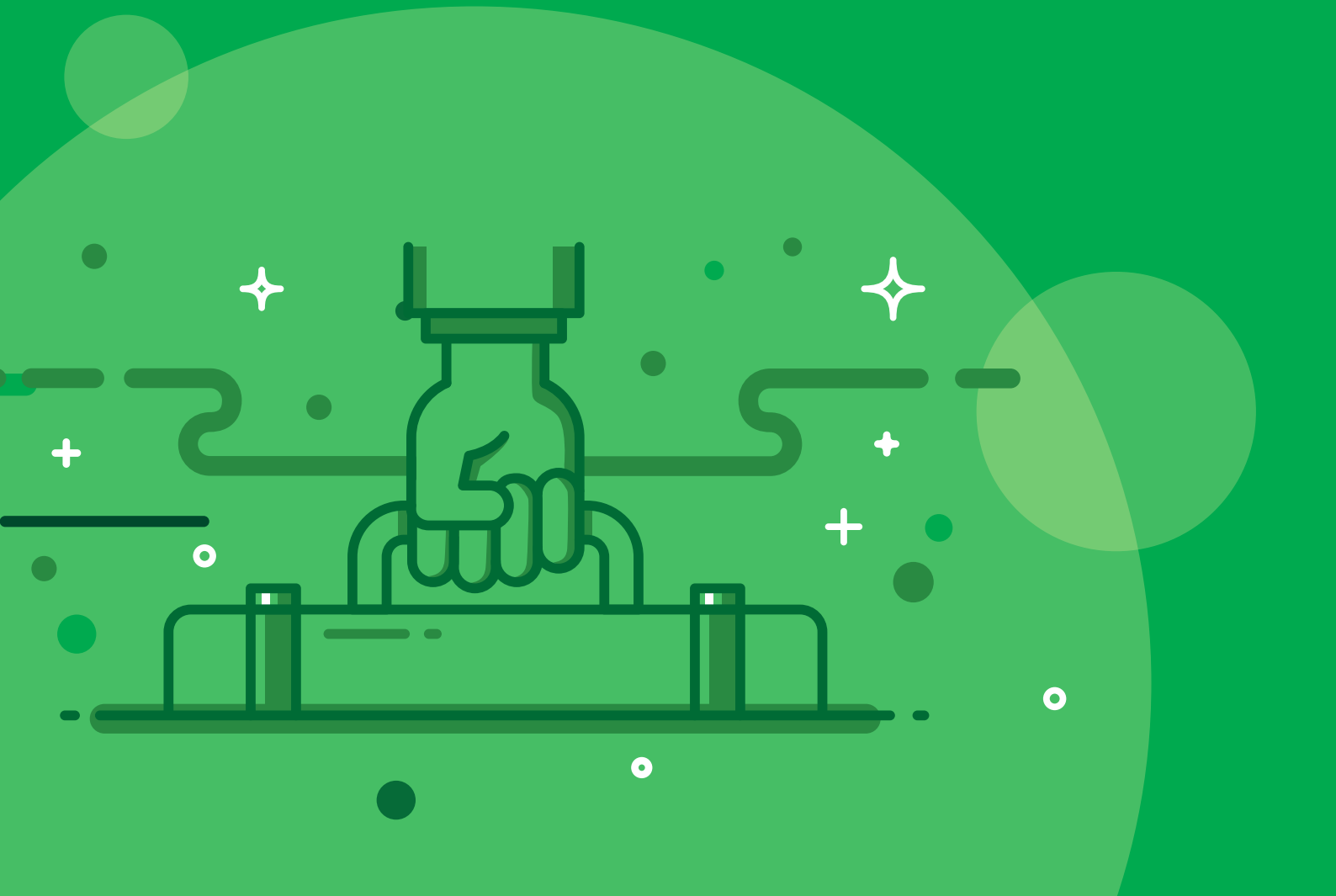
Periodic testing:
It validates that the system is performing as expected and assess its effectiveness in managing specific risks.

Robust investigation process:
With screening systems generating a significant volume of alerts, allocating adequate resources to implement and maintain a sanctions programme is essential. This task should be supported by a detailed investigation and a robust workflow process (to escalate and close alerts, and maintain an audit trail of the decisions taken).

[4] Source: Deloitte report : Facing the sanctions challenge in financial services

Section 4

Trade-based money laundering continues to pose challenges



The international trade system provides criminal organisations an opportunity to launder the proceeds of crime with a relatively low risk of detection (as money being laundered can be seen coming through legitimate trade transactions). This is facilitated as these criminal organisations hide their activities amongst massive volumes of legitimate trade that is difficult to discover. Techniques such as under- or over-invoicing and falsifying documents, can be difficult to trace as they can involve multiple parties, jurisdictions, and transactions. These techniques are also compounded by lack of systemic exchange of customs data amongst countries.

While controls can be put in place for documented trade, challenges lie in open account situations where banks/FIs have little or no visibility on the underlying transaction. TBML is difficult to spot because it tends to be hidden amongst legitimate transactions or activity. It often involves genuine trade and the associated paperwork, with only the subtlest of clues hidden deep in the trade structure or trading histories to indicate suspicion that is compounded by lack of data to identify red flags.

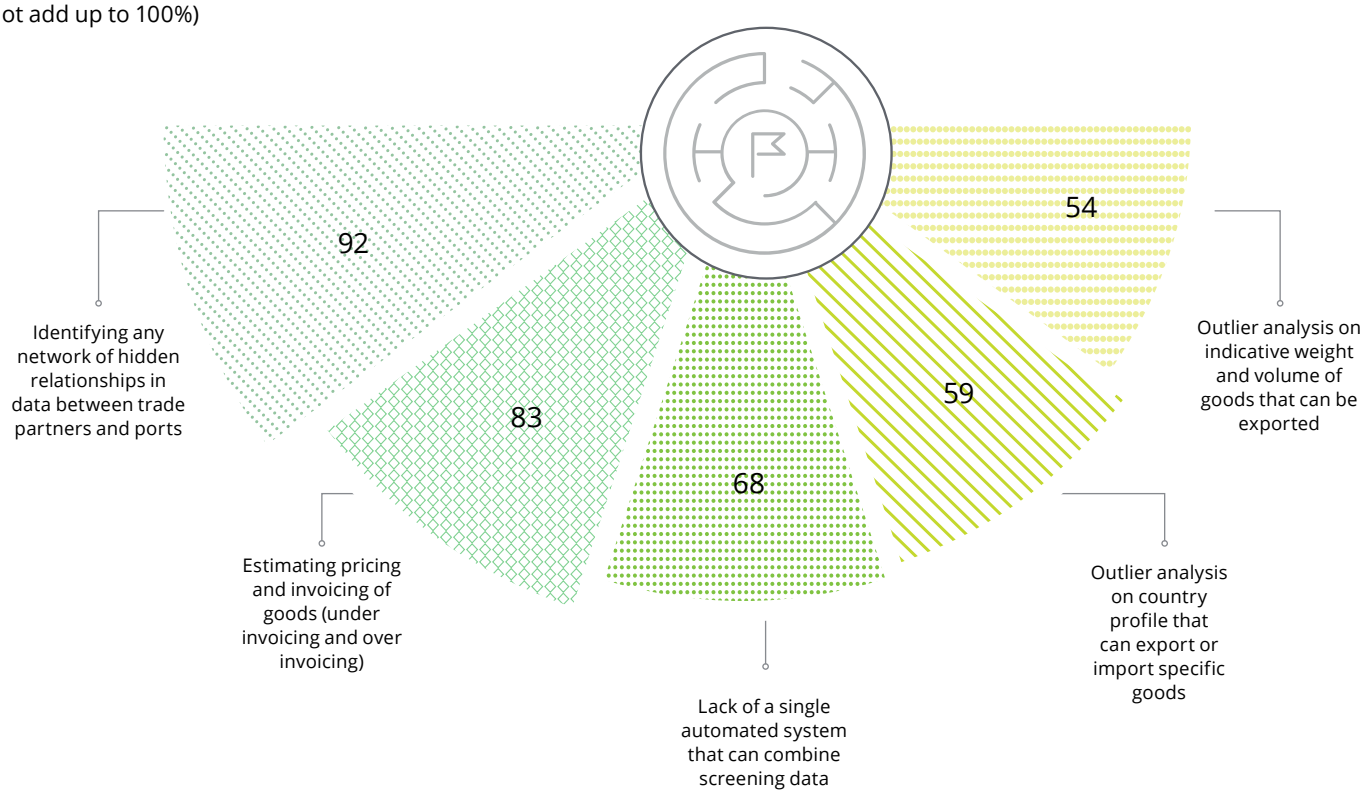
Over the years, regulators and standard setting agencies categorised trade finance as a "higher-risk" business for money laundering, terrorist financing, and potential breach of sanctions.

Increasing complexities and trade flow volume creates opportunities for criminal organisations to launder proceeds of crime through the international trade system. Consequentially, FIs have been facing difficulty in monitoring and implementing controls in their trade finance business to combat TBML. The problem has been further exacerbated by lack of clarity in the compliance requirements and regulatory expectations in many jurisdictions.[6]

Per FATF recommendations, the specific measures to combat TBML should include (at the minimum) the following:

- Assessing the adequacy of a bank's framework to manage the risks associated with trade finance activities, including whether the bank effectively identifies and monitors its trade finance portfolio and the controls around it
- Incorporating systems and process to determine how a bank monitors trade finance activities for any suspicious transactions and reporting (based on the bank's risk assessment of its size, complexity, location, and types of customer relationships)
- Providing AML training to financial institutions' global trade services departments and people

As part of processing trade finance or trade-based transactions, in which of the following areas have you experienced challenges? Please tick all that apply. (This is a multiple choice question. Responses will not add up to 100%)

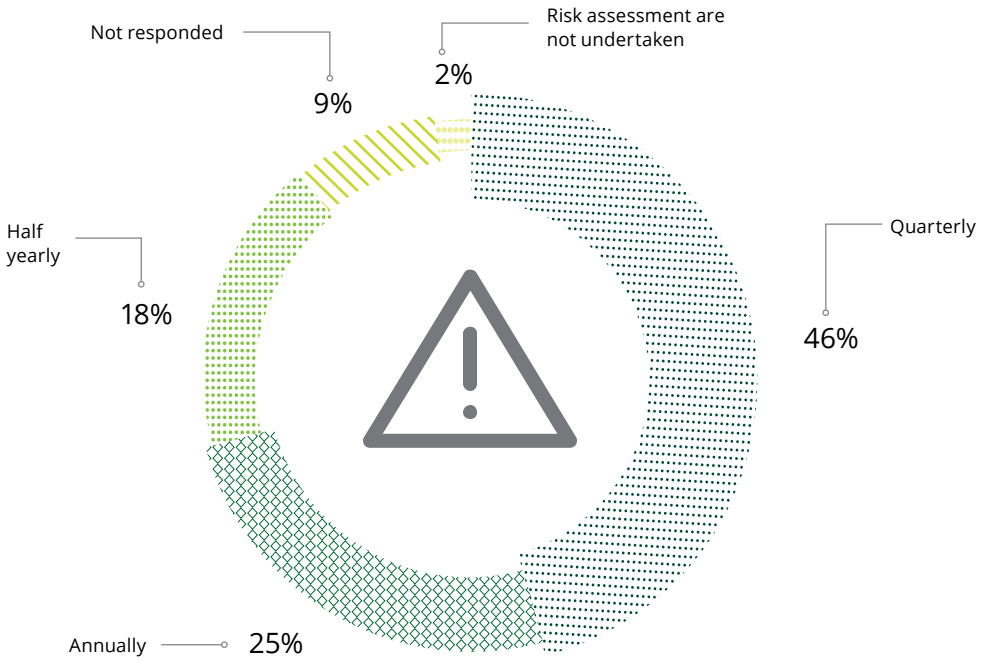


[6] Source: https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/financial-services/sea-fsi-tbml-compliance.pdf

Combating TBML – Moving forward

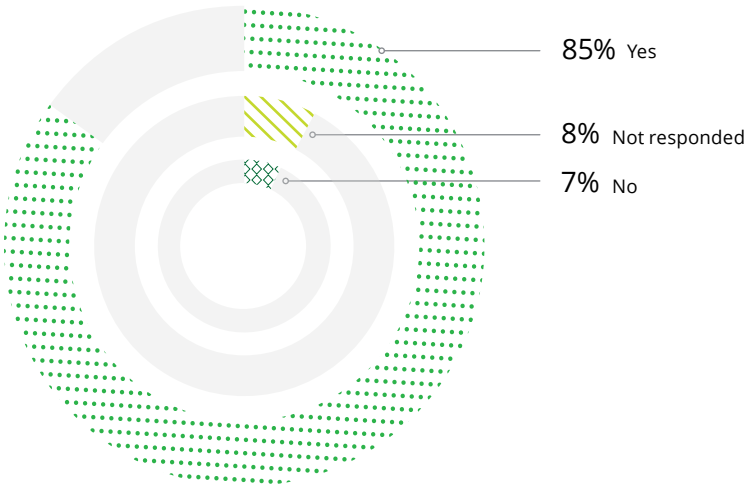
Given the intense focus on TBML across the world, banks should undertake a comprehensive risk assessment of their trade finance business taking into account their customers, geographical locations, and products and services offered. This should, at the minimum, include controls with a specific focus on customer due diligence procedures, transaction screening, and document review and screening. An overwhelming 88 percent respondents indicated that they undertook risk assessment; almost 46 percent of them indicated that they do this every quarter.

How often are risk assessments undertaken in your trade finance business?



Given the limited amenability of automation of the TBML scenario, banks must have a sound compliance programme in place. Regular training must take place to identify red flags, such as improperly modified documents, use of vessels inappropriate for type or volume of goods, inconsistent transport documents, and over valuation of goods. An overwhelming 85 percent respondents have indicated that they provided TBML specific training for their staff.

Is a tailored training on AML risks provided to your trade finance teams?



Changing landscape of trade finance monitoring

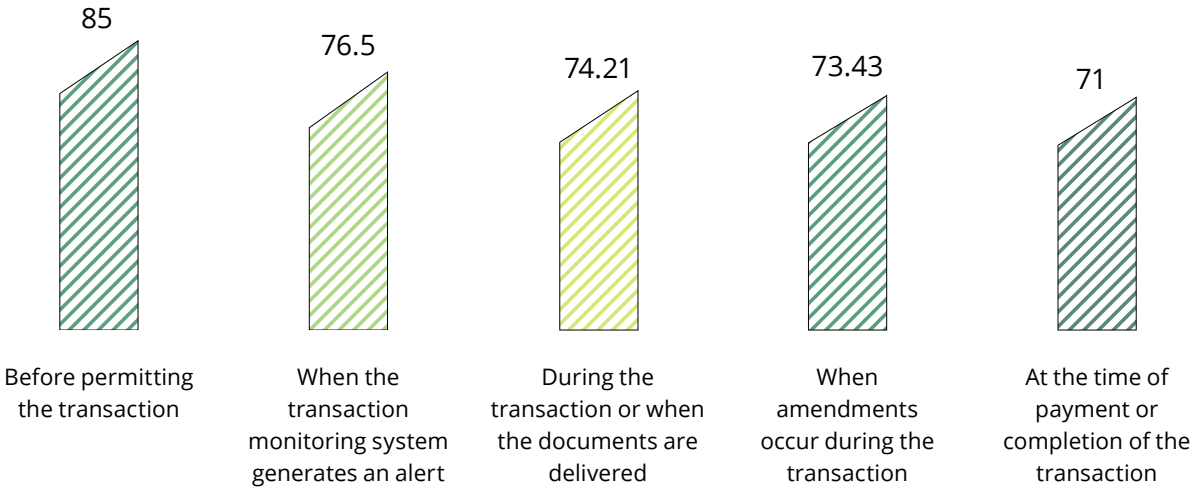
Regulatory demand for compliance places pressure on business processes. This is particularly difficult in trade finance due to the need to comply with various regulations imposed by different jurisdictions. The KYC process and regulation to enforce embargoes continue to place a heavy load on trade bankers.

Until recently, compliance in trade finance was limited to the examination of documents. The traditional view was that fraud is the main risk within trade finance. Now, in addition to document review, there is expectation of extensive screening against multiple lists of data elements embedded in ancillary documents with risks classified into three categories – embargoes; TF (including fraud); and sanctions/proliferation financing. An overwhelming 85 percent respondents indicated that the transactions are screened against banks' internal, regulatory (prohibited goods), and sanctions lists.

Are trade finance transactions screened against your internal, regulatory (prohibited goods), and sanctions lists?

Regulatory bodies expect that banks should undertake pre- and post-transaction screening to ensure screening at every step of the transaction and review of the documentation for anomalies or "red flags". Screening elements include customers and their details (including address, jurisdictions, stakeholders, and beneficial owners), types of trade finance contracts, and contract parties (including shipping and insurance companies, and contracted goods and services). The screening should be done at every stage of the trade finance process, including when any amendments to the document are made. About 85 percent respondents indicated that they screened trade finance transactions before permitting the transaction. However, only 73 percent respondents screen the transaction when documents undergo any amendment.

At what stages do you screen your trade finance transactions? Please select all that apply.



Key challenges in TBML monitoring

Over the past few years, standards setters, such as FATF and industry groups (such as Bankers Association for Finance and Trade, BAFT, and Banking Commission of the International Chamber of Commerce, ICC), and Wolfsberg Group have provided thought leadership and guidance on international standards or best practices to combat TBML. These are best practices that will need a push from local legislation or regulation makers.

In our experience, some of the common red flags to ascertain TBML are given below:

Customer red flags
Engaging in transactions that deviate from the regular business strategy or those lacking apparent business sense; for example, a steel company started dealing in sugar and paper products frequently

Document red flags
Abnormality in documentation commonly required in trade finance that includes letter of credit (LC) and bill of lading; incomplete or dubious documents may warrant increased scrutiny and due diligence effort; for example, shipment locations of goods inconsistent with those mentioned in LC; actual shipments occur in high-risk countries

Transaction red flags
Specific transaction terms and structure that are incoherent with industrial norms and do not make economic sense; for example, a request to include clauses that seek to benefit buyer/seller and a complex transaction structure across numerous intermediaries without supporting reasons

Payment red flags
Unusual or complex payment terms that may involve specific clauses to obscure the true identity of the ultimate beneficiary; for example, a request to pay third party in cash, payment in tax haven, or high banking secrecy jurisdiction

Shipment red flags
Concerns about the nature and characteristics of actual goods to be shipped/received, particularly if the shipping method does not make economic sense or is highly unlikely due to weight/quantity/value of goods; for example, using a 40 ft. container to transport a small amount of low-value goods

[7] Source: https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/financial-services/sg-fsi-seminar-2016-radish-singh-emerging-trends-solutions-aml-cft-noexp.pdf

Further, to address the challenges of determining fair pricing, import-export licences, circumvention, etc., banks and FIs may consider the following suggestions:[8]

Ascertaining the right price
Intrusive price checks may not be an automatic action in cases (1) where the customer is a known/reputable business or (2) has a long-standing relationship with FI or (3) the price variation is within the acceptable range (based on standards developed using the bank's own transaction data). Banks may also establish their own internal databases for price guidance based on the transactions they manage.

Know the goods transacted
Trade documents do not provide a detailed description of goods or components. A good practice is to usually screen goods (using preferably a paid database) to ascertain whether they have dual use. This can then be matched with the bank's customer profile and knowledge (where information should have been gathered at the onset on the goods intended to be traded), details of the transactions conducted by the customer and parties involved, length of the relationship, and the issues seen during the lifecycle of the customer. Banks may need to take a heightened risk approach with a new customer relationship where the goods traded are capable of dual use.

Import/export licensing
Banks are usually not in a position to determine if an export licence is required for a trade transaction. At best, they can seek advice on typical goods requiring such licences in their key jurisdictions via their customers and transactions. They can also seek their customers' confirmation that where required, such a licence has been obtained.

Circumvention
Regardless of the checks conducted and controls put in place, banks may find it difficult to confirm that a customer is involved in circumvention. When a trade ends at a port of discharge on paper (which is confirmed by end of the vessel route), it is quite a challenge to ascertain that goods were transported later to a sanctioned, or a high-risk jurisdiction or party, or otherwise routed to jurisdictions where there are restrictions placed on certain goods. In such a situation, the potential use of tug boats and feeder vessels makes ascertaining circumvention more complex. Banks can only make best efforts to make enquiries to confirm that there is no suspicion of circumvention in a case where a customer trade ends at a port or jurisdiction known (based on experience) for circumvention, neighbouring a sanctioned or high-risk country or a country where certain goods are restricted or where there is suspicion of transhipment without a good reason.

Data availability and quality
Despite the level of technology available, trade finance processes continue to be largely paper-based. This makes it challenging to have a holistic view of information flows in trade transactions. In the near-term, banks may consider implementing Optical Character Recognition (OCR) capabilities in the trade finance process. This can make scanned text computer readable. OCR may help extract relevant information and store that in the electronic form. Analytics tools may be used to check the data for anomalies, red flags, and trends.

Detecting duplicate LCs, bills of lading (BL), and invoices
Although knowing if a customer is submitting a duplicate or fraudulent trade document is challenging, banks may cross-check with the issuing bank when presented with trade documents. Relying on a MT700 message alone may not suffice. If multiple banks seek confirmation from the issuing bank, a red flag review should be triggered by the issuing bank (that can alert other banks and take a necessary action).

[8] https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/financial-services/sea-fsi-tbml-compliance.pdf

About the survey

This survey report has been developed on the basis of responses received to a survey questionnaire circulated to leading banks and FIs in India, Sri Lanka, and Bangladesh from January–March 2020. We received 126 responses from banks in these three countries and engaged iResearch Services to collect the survey data.

The response rate to questions varies and not all respondents have answered all questions in their respective surveys. Each statistic used in this report is derived from the number of responses to that question and must not be considered consistent across the report. For multiple choice questions and priority-based questions, the weighted average of responses for that question has been used to derive the statistics.

The report considers consolidated findings across countries. Country-specific charts are provided in the subsequent pages for reference.

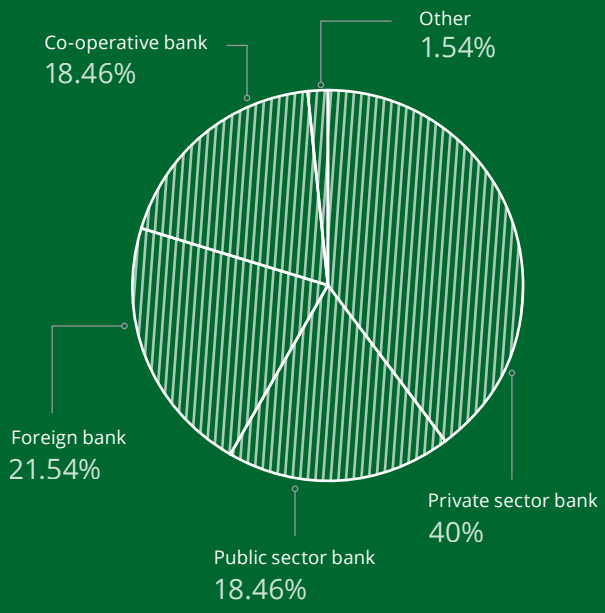
Acknowledgement

Amol Mhapankar
Darpan More
Manish Mandhyan
Rajesh Chawla
Soniya Mahajan

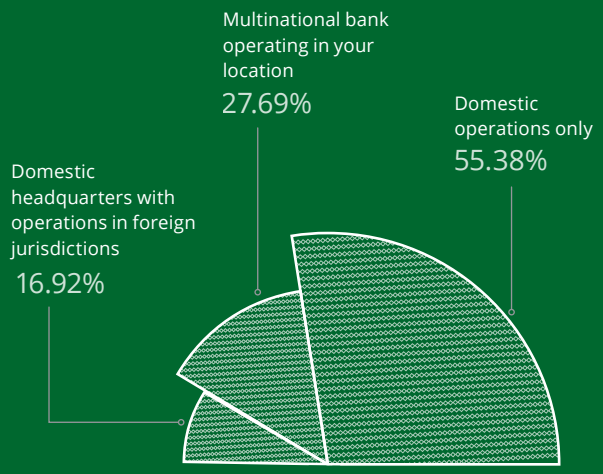
Country-specific findings

India charts

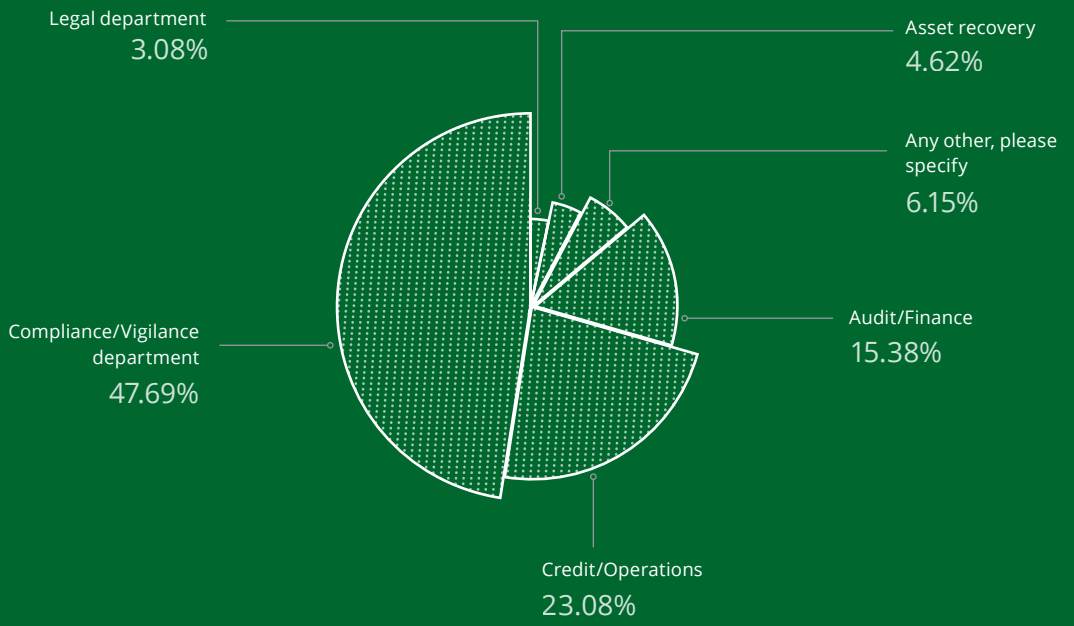
What is the type of bank you are representing?



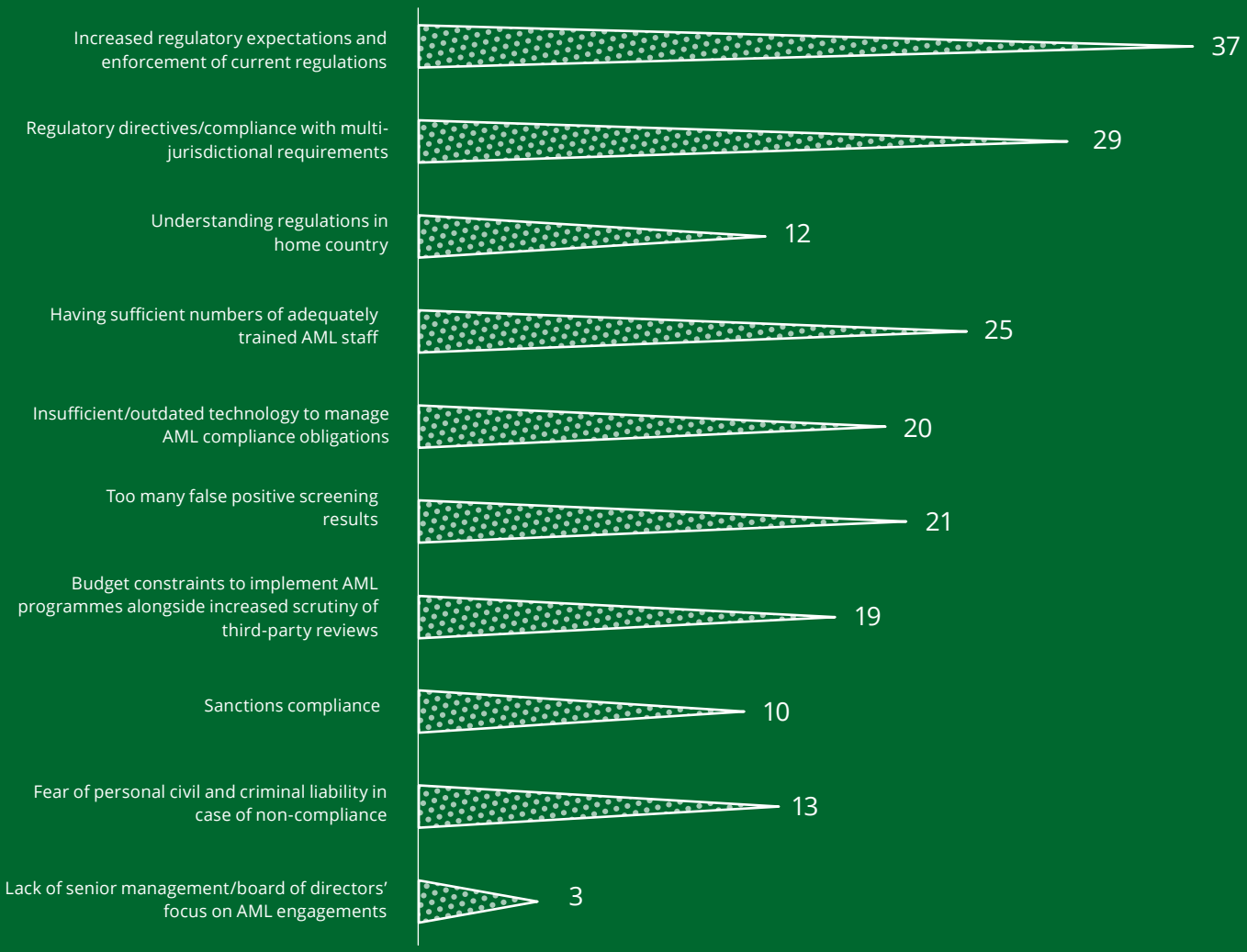
What is the scope of your bank's operations?



Which department do you belong to within your bank?

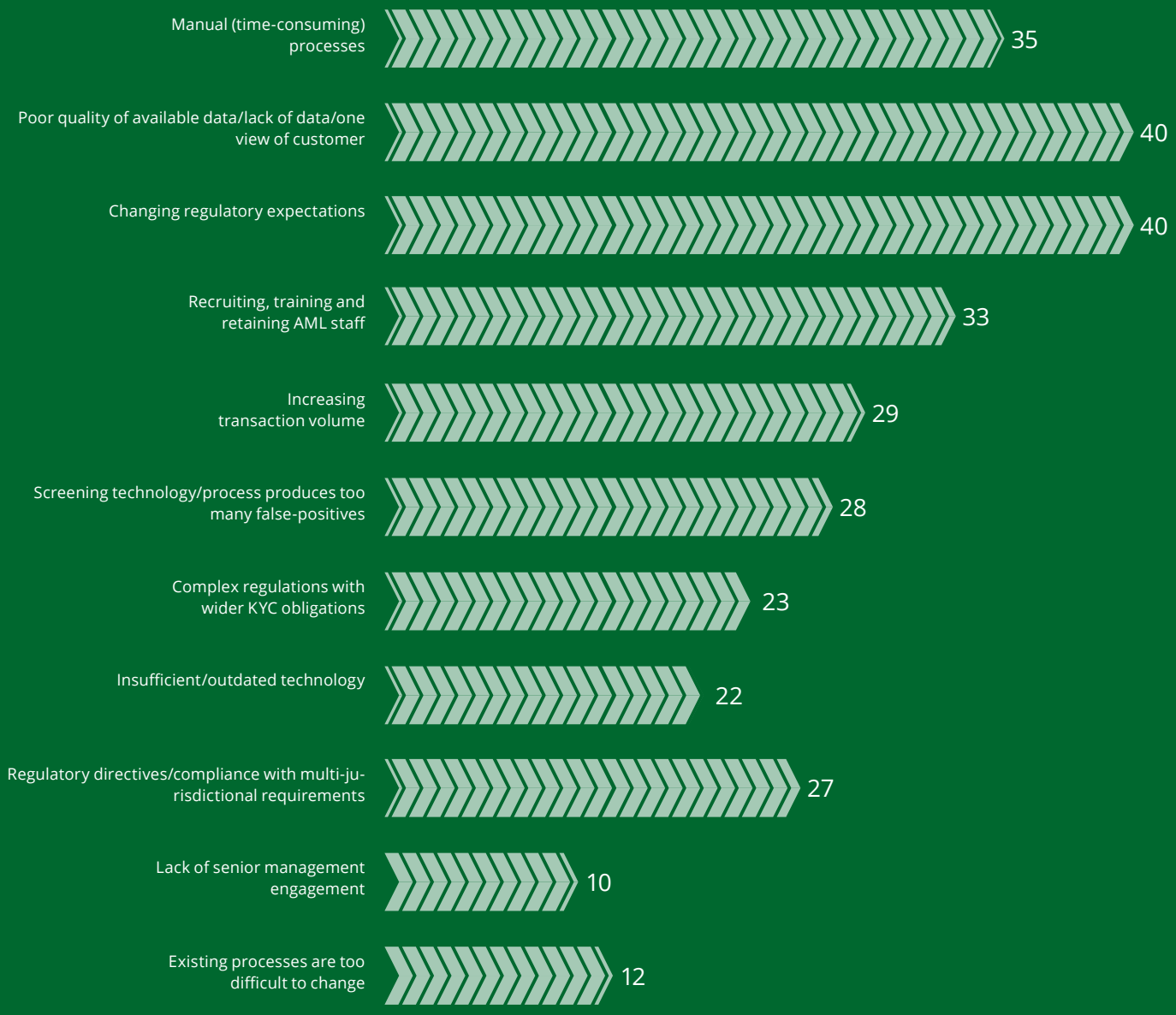


According to you, what are the biggest AML compliance challenges that banks face currently? Select the top three options.

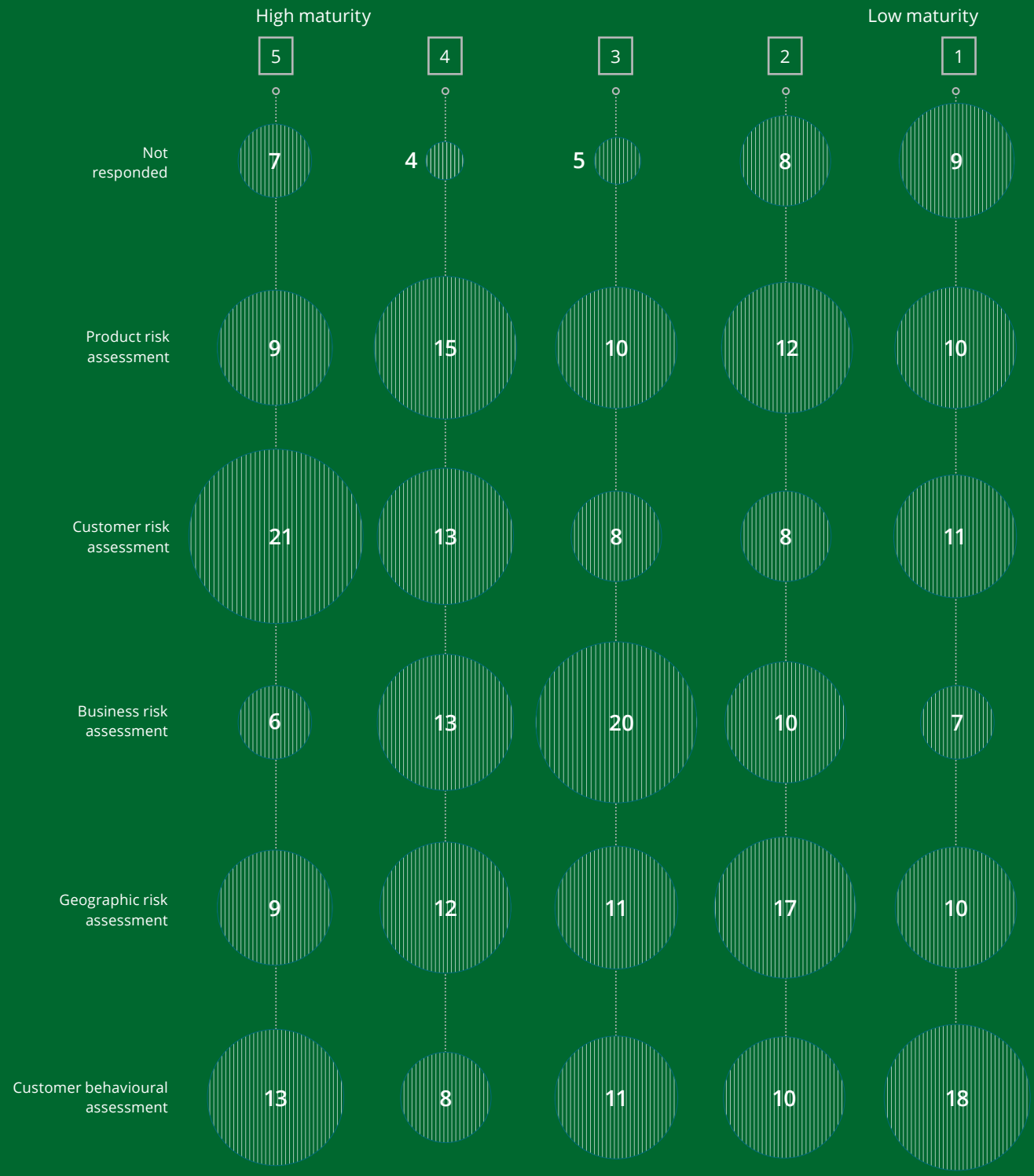


Please indicate which measures you have in place to manage AML and sanctions compliance.

Please identify the top five operational challenges faced by your organization in complying with AML regulations.



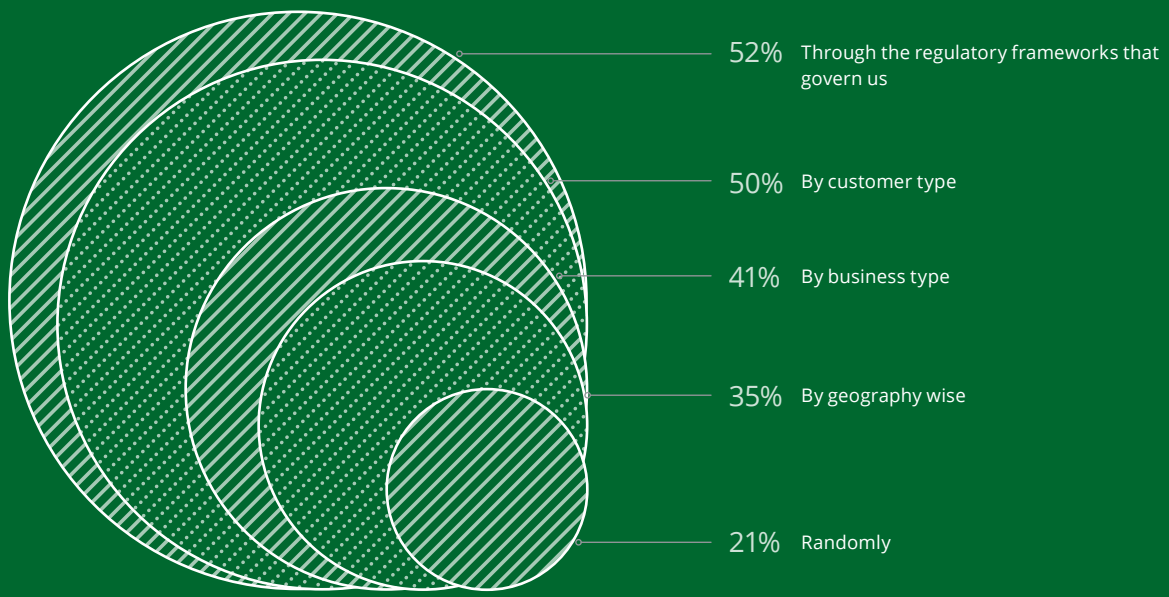
Please rate the following components of the AML programme in terms of their maturity in your organisation. (1 = low maturity and 5 = high maturity)



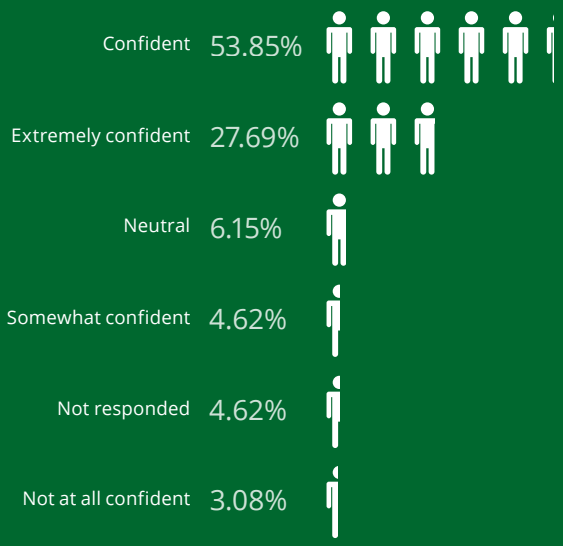
Please indicate if the following statements are true or false.

	True	False	Unsure	Not respoded
In my organisation, senior management/ board of directors take an active interest in AML issues by discussing them formally at senior management/board meetings.	61	3		1
In my organisation, the AML programme has been identified as strategic priority.	56	3	5	1
My organisation has allocated adequate funding to develop and operate our AML programme.	54	5	4	2
My organisation has an enterprise-wide view of our risk exposures to potential money laundering.	54	4	5	2

How does your group address your risk exposure to money laundering? Please select all options that apply.

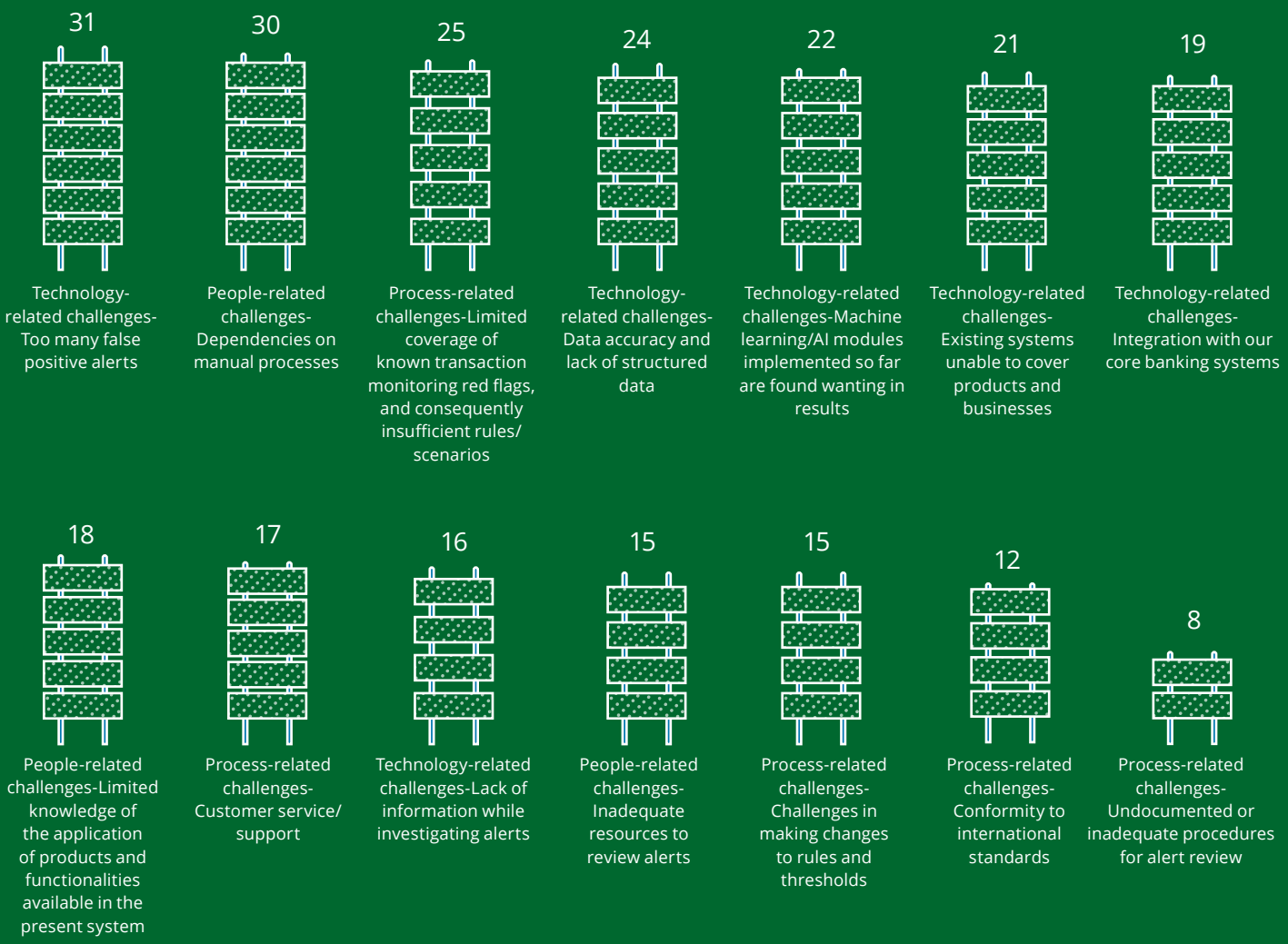


How confident are you that your financial crimes prevention/framework is compliant with all regulatory requirements and expectations?

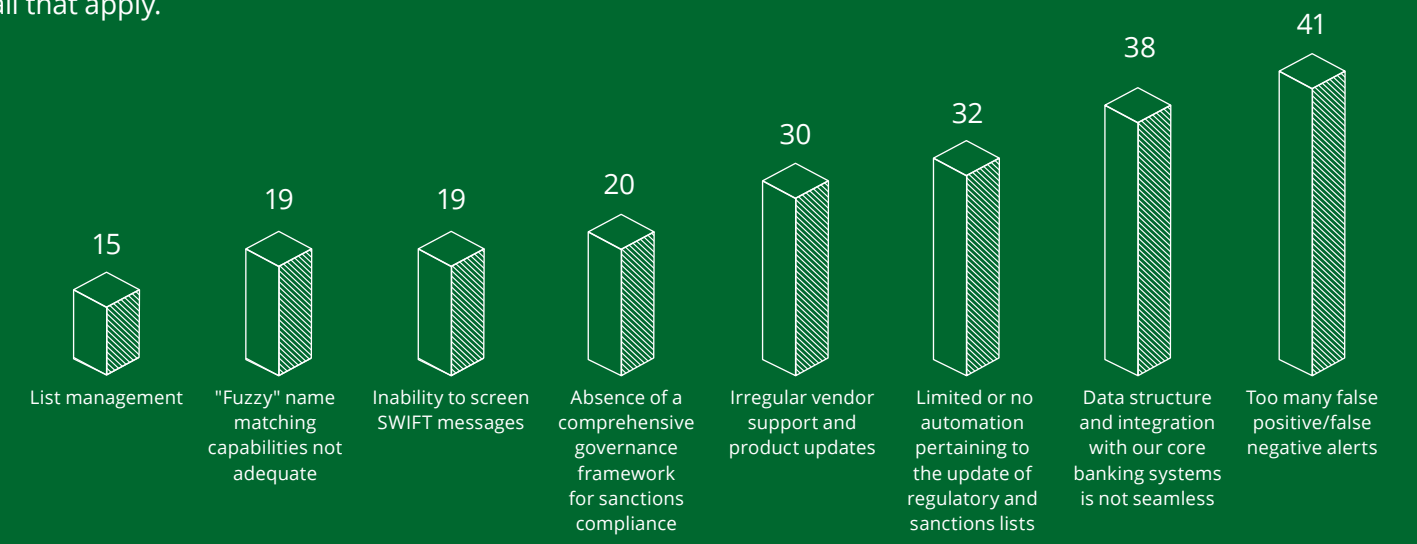


Where do you believe banks need to focus for better AML compliance in the next two years? Select the top three options that apply.

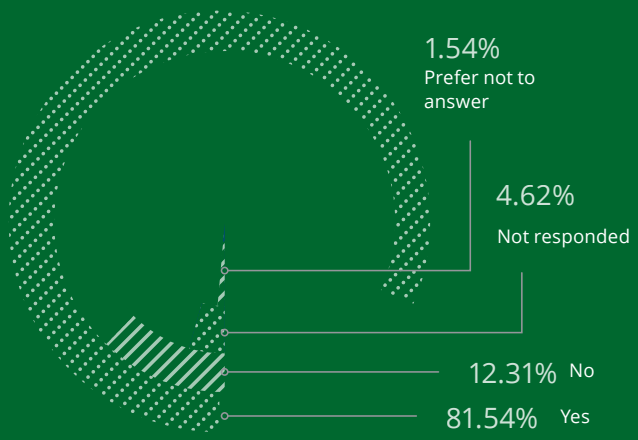
What are the biggest challenges with your current transaction monitoring system? Identify the top five challenges across categories.



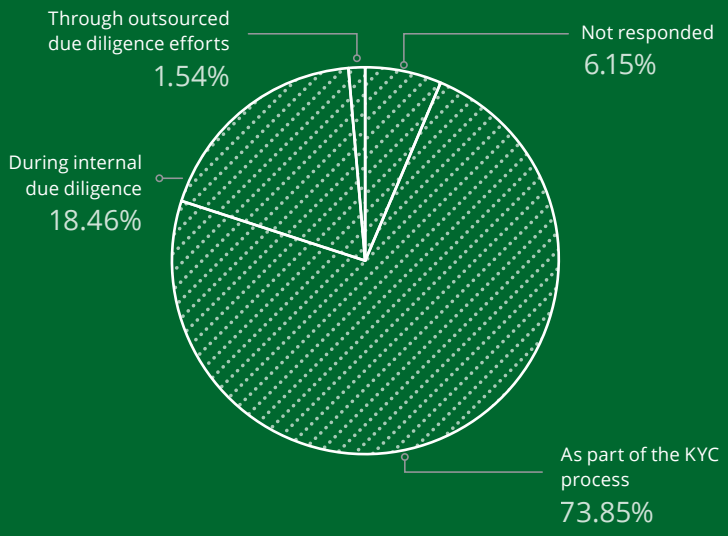
What are the factors that are affecting your confidence in your current screening solution? Tick all that apply.



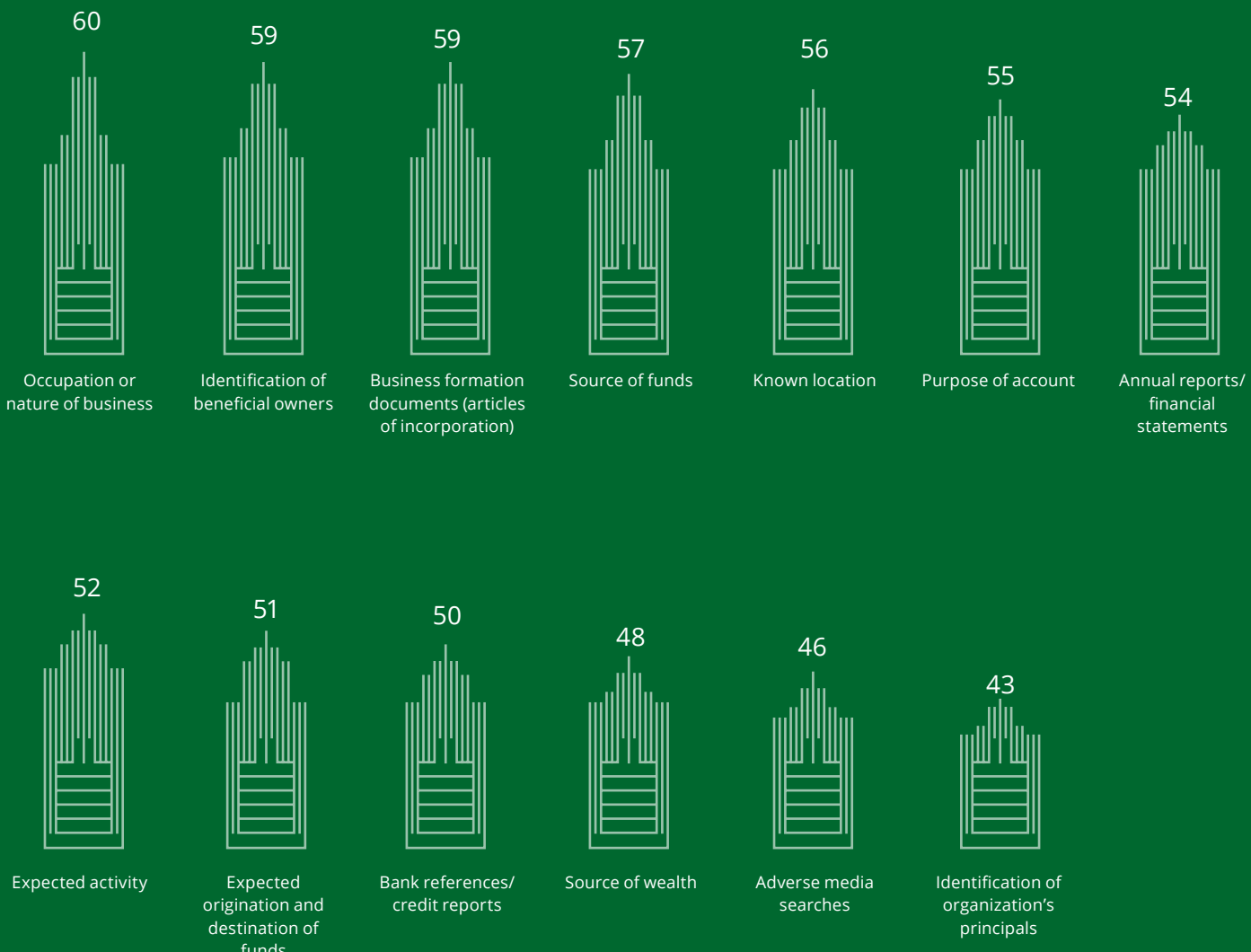
As part of the name screening process, do you also screen for politically exposed persons (PEPs)?



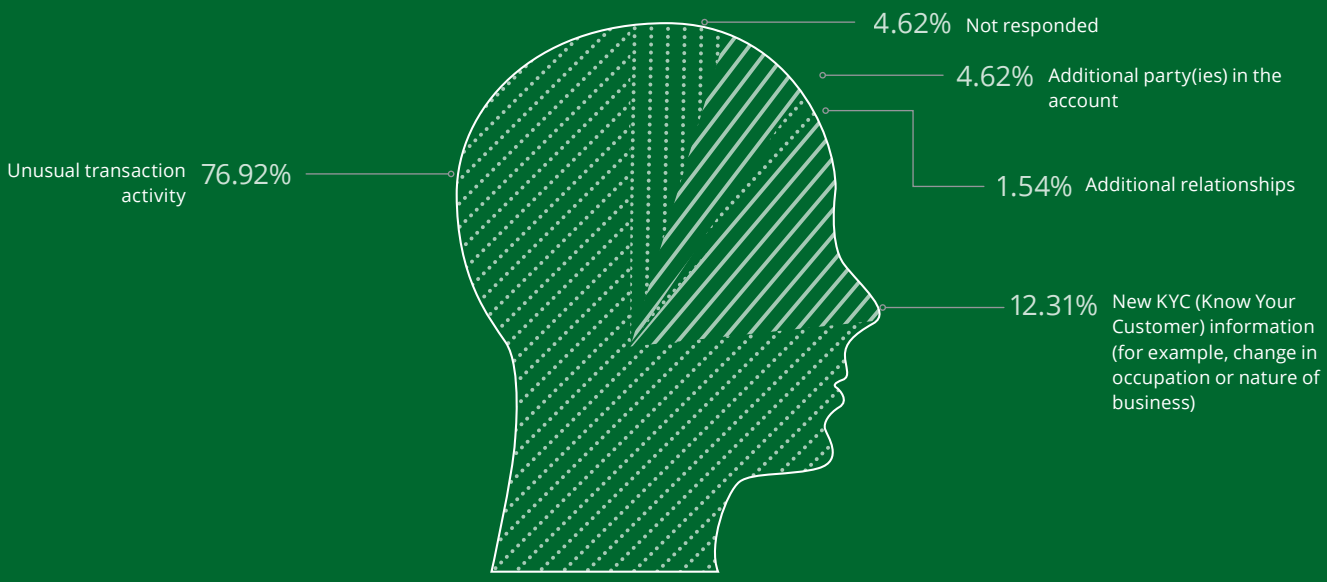
How is beneficial ownership verified in your organisation?



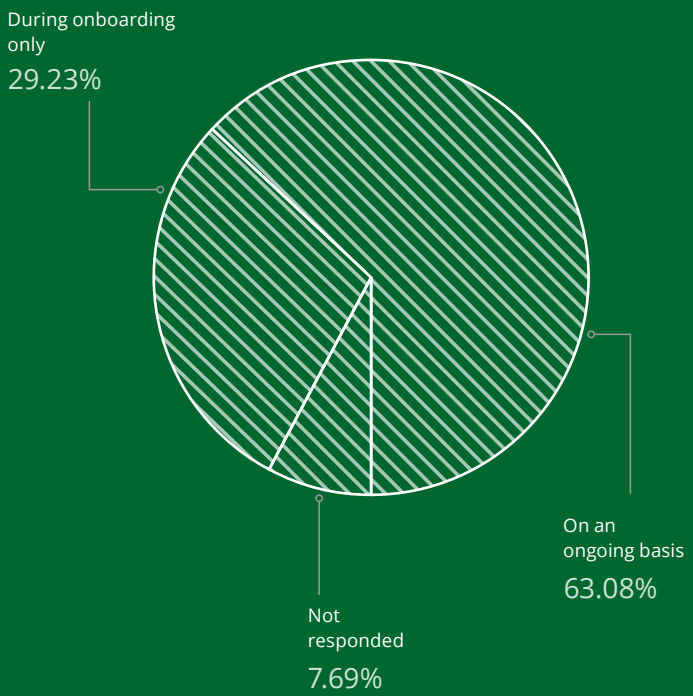
Which of the following types of information does your organization currently gather as part of its CDD process? Tick all options that apply.



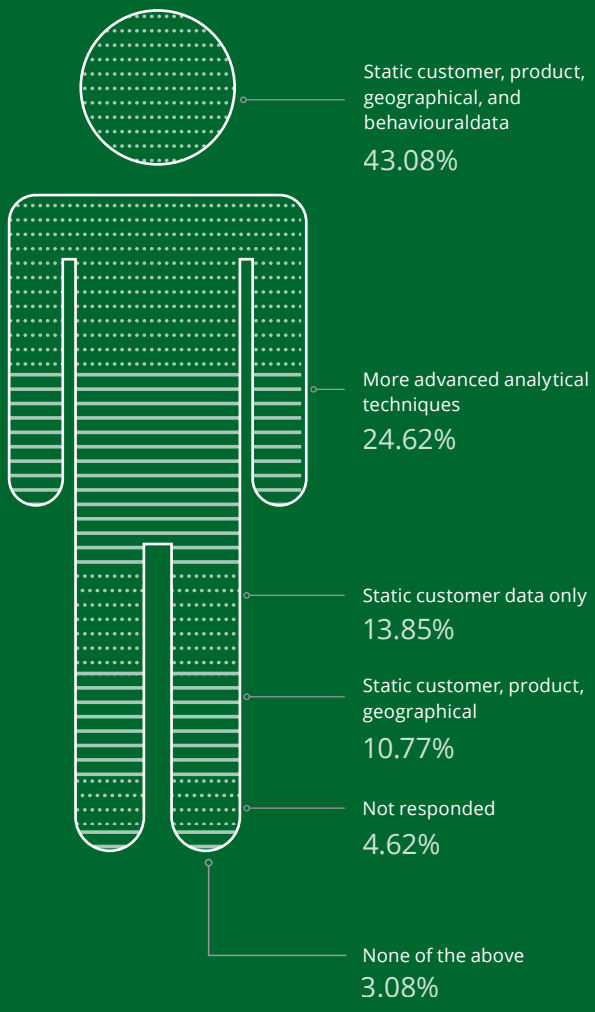
In your view, what would trigger a review or update?



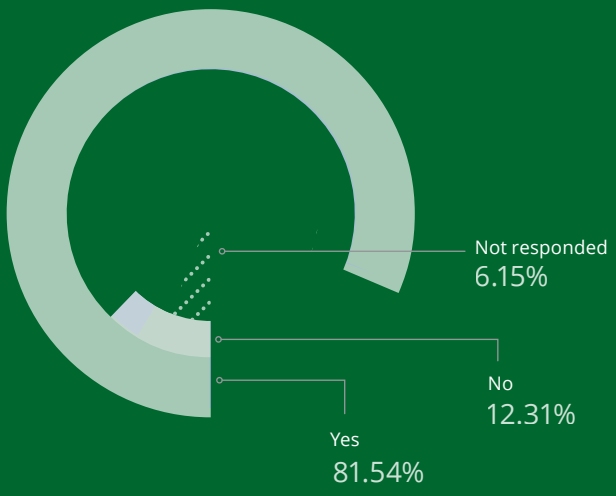
When are adverse media searches performed?



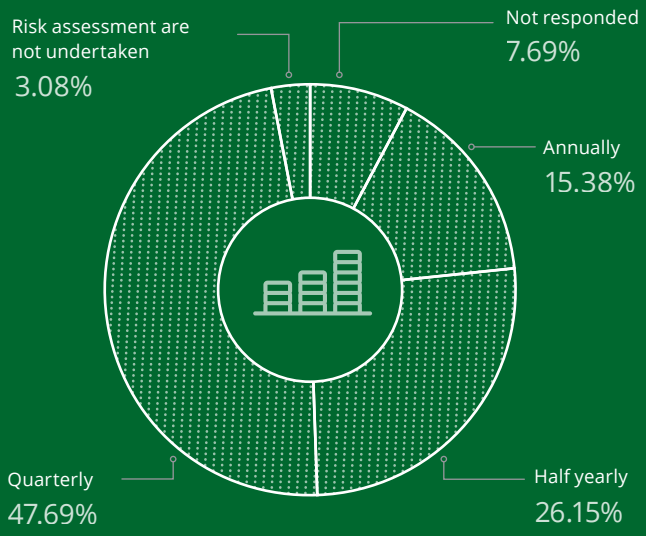
What factors are incorporated in your customer risk rating algorithm?



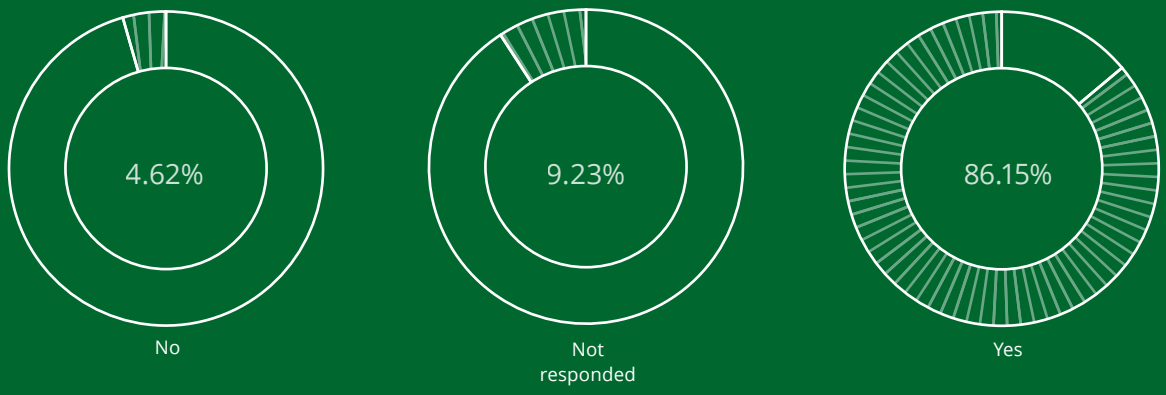
Is a tailored training on AML risks provided to your trade finance teams?



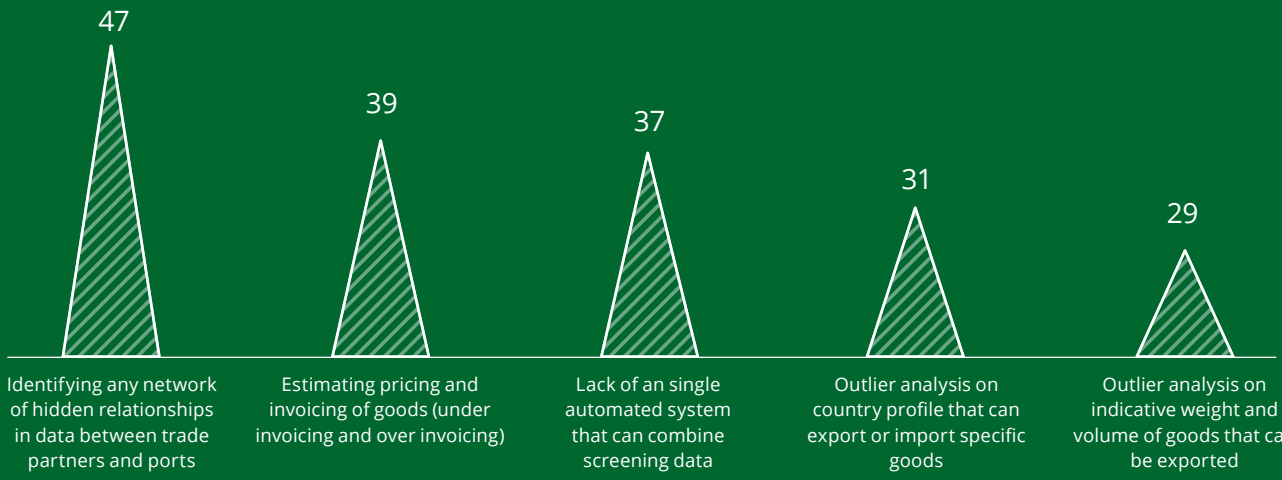
How often are risk assessments undertaken in your trade finance business?



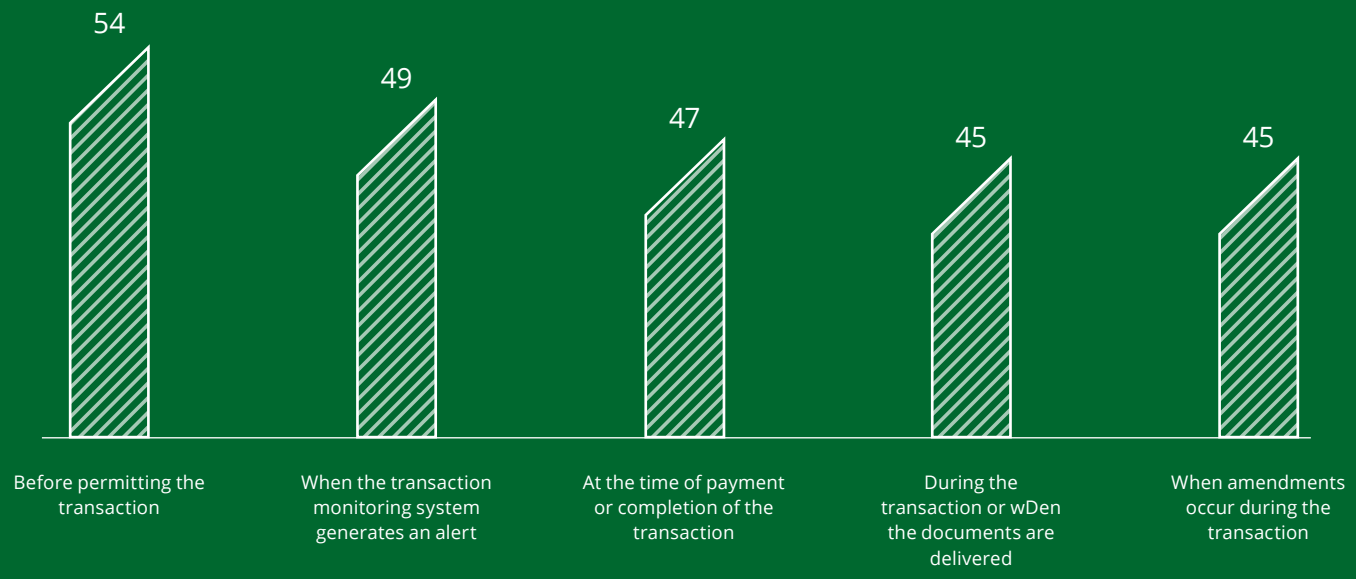
Are trade finance transactions screened against your internal, regulatory (prohibited goods), and sanctions lists?



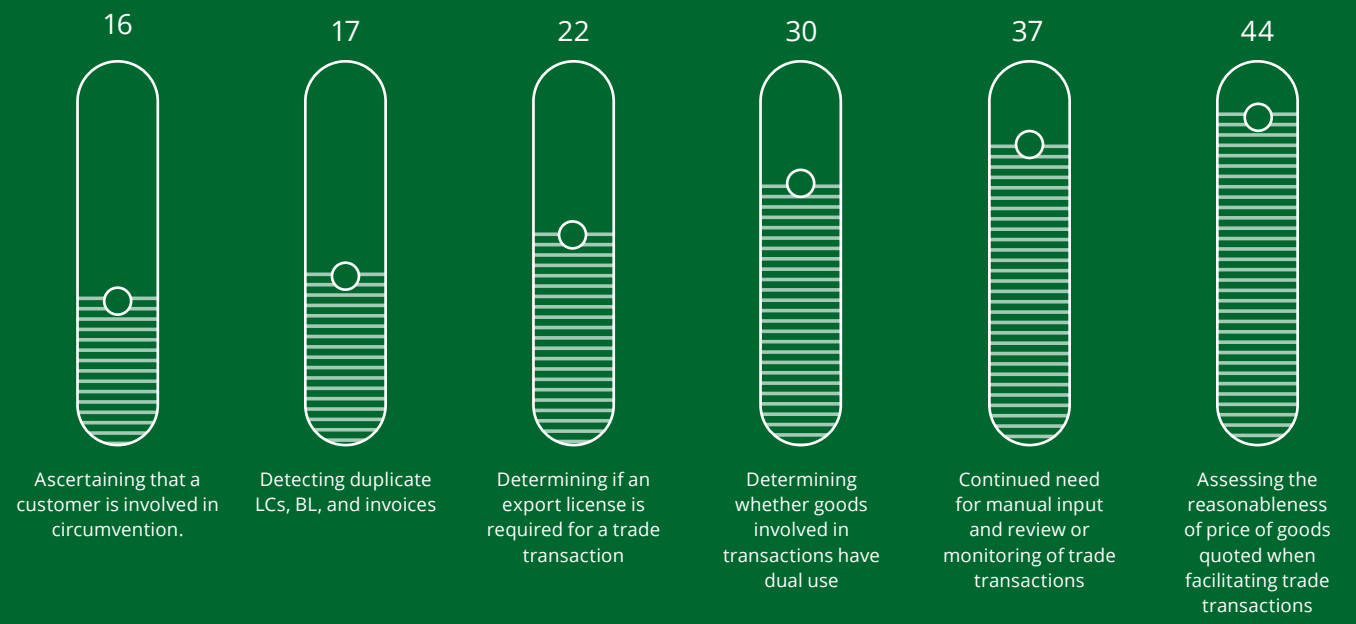
As part of processing trade finance or trade-based transactions, which of the following areas have you experienced challenges? Please tick all options that apply.



At what stages, do you screen your trade finance transactions? Please select all options that apply.

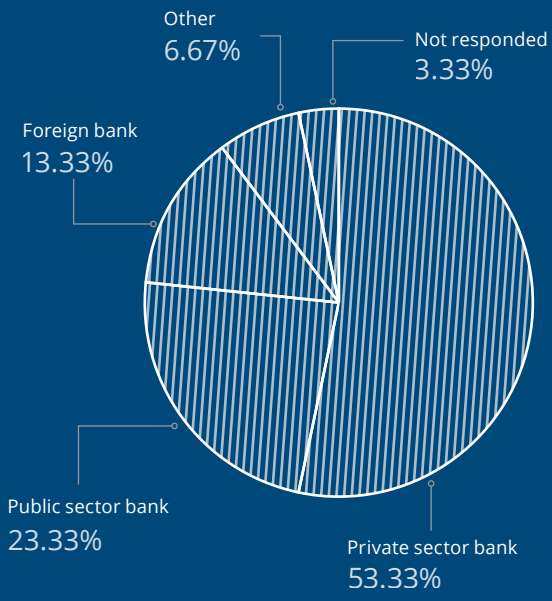


What are your biggest challenges when it comes to detecting TBML red flags? Select the top three options that apply.

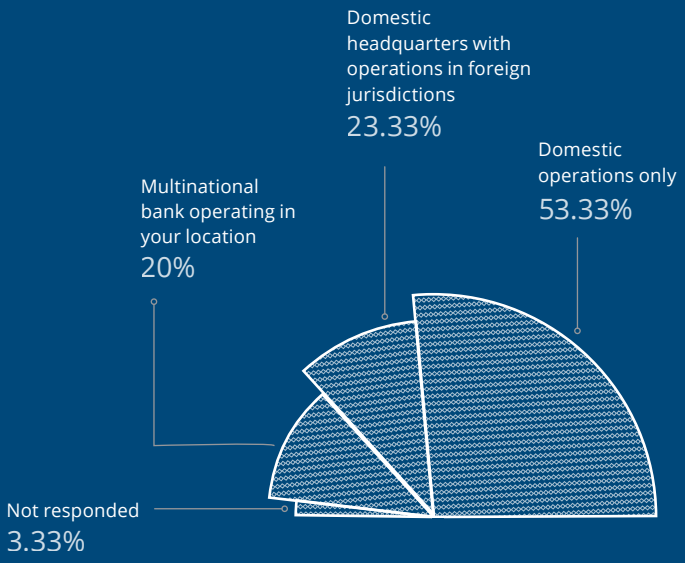


Sri Lanka charts

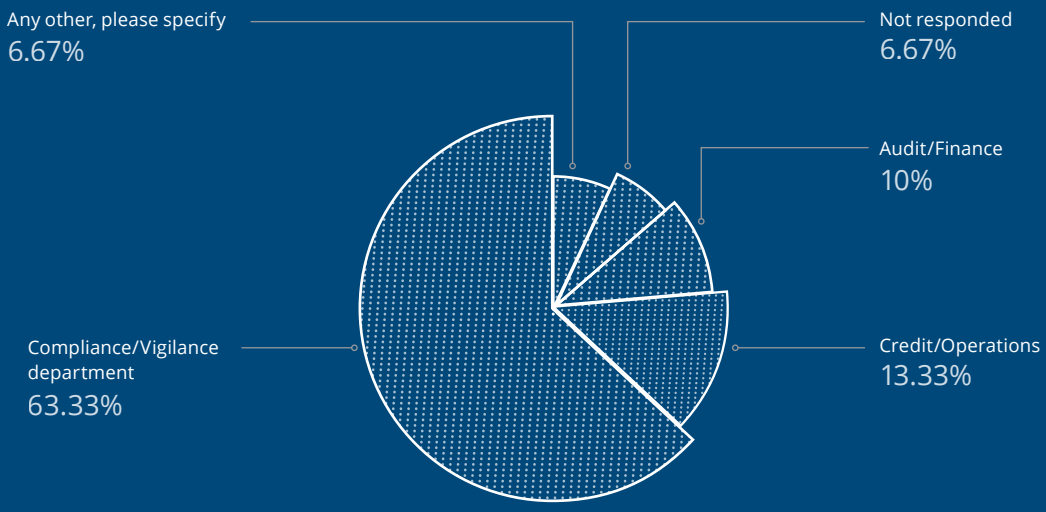
What is the type of bank you are representing?



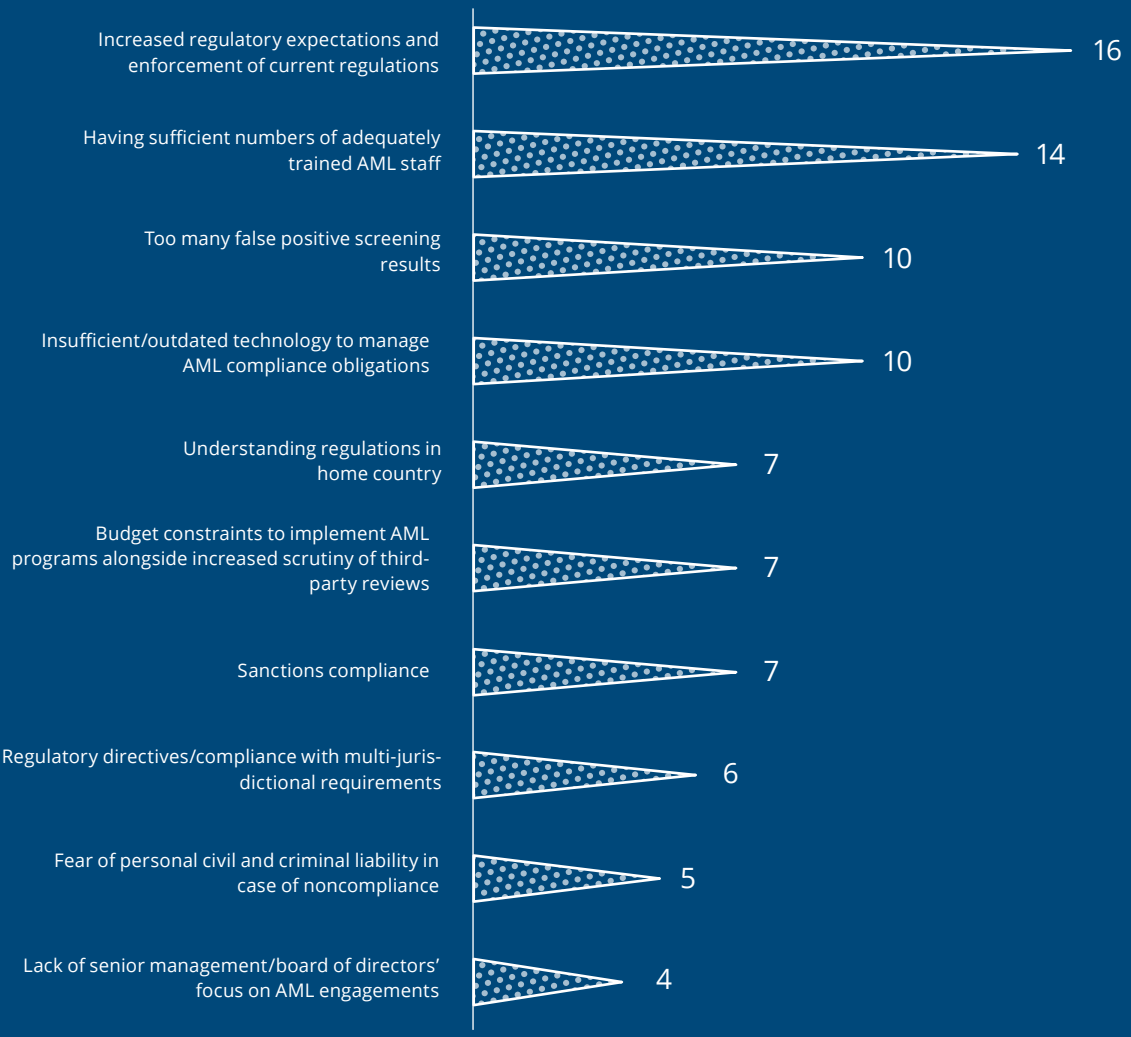
What is the scope of your bank's operations?



Which department do you belong to within your bank?



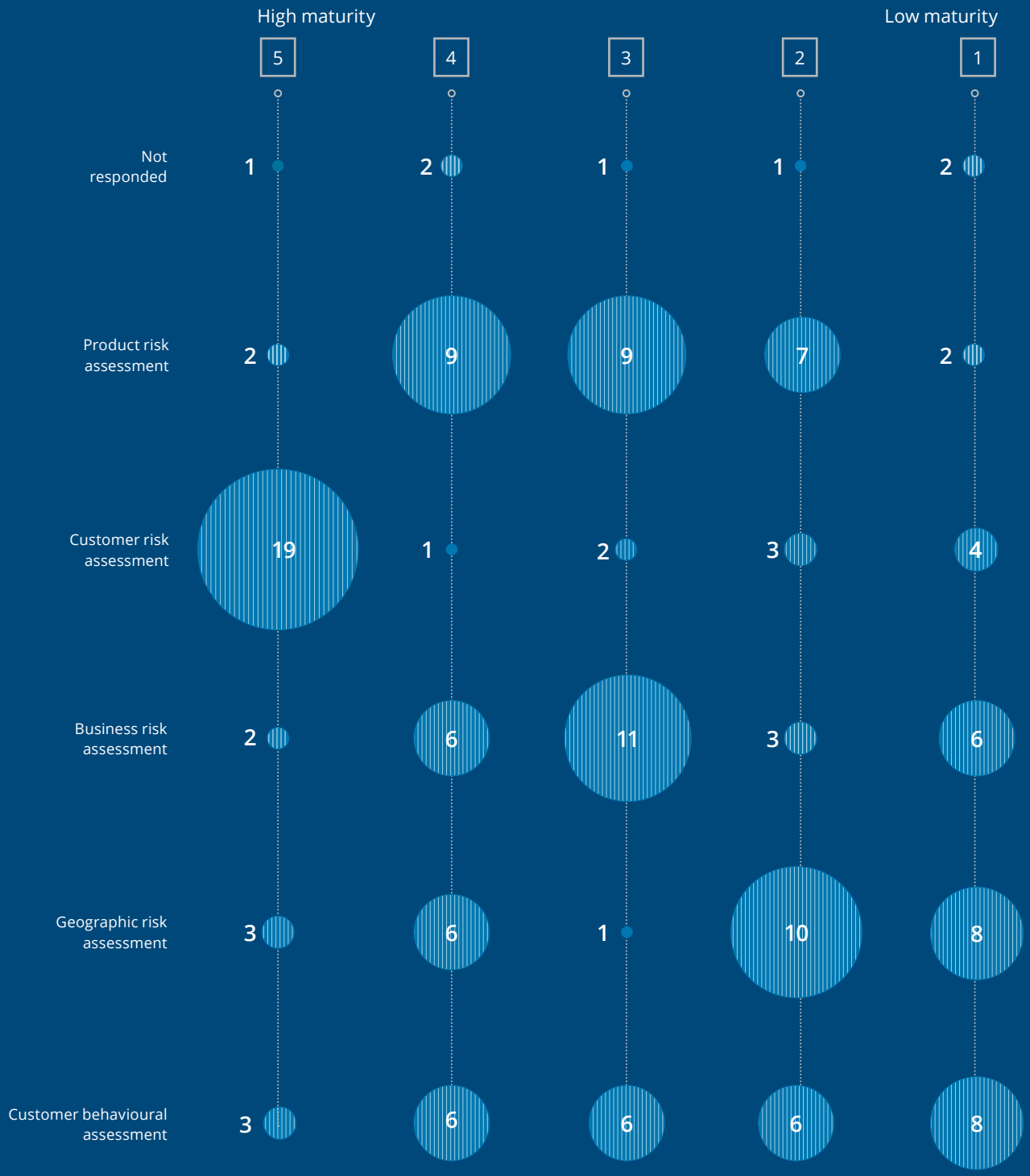
According to you, what are the biggest AML compliance challenges that banks face currently? Select the top three options.



Please identify the top five operational challenges faced by your organization in complying with AML regulations.

Please identify the top five operational challenges that your organisation faces while complying with AML regulations.

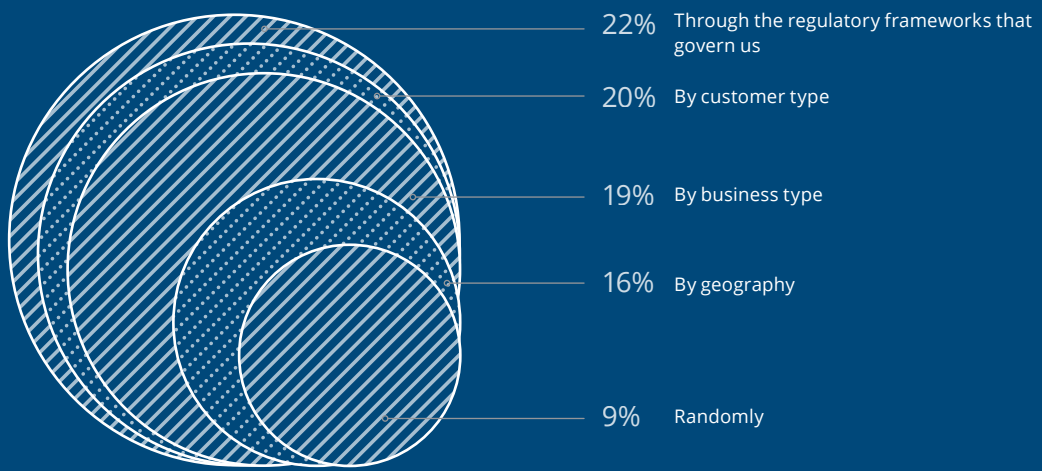
Please rate the following components of the AML programme in terms of their maturity in your organisation. (1 = low maturity and 5 = high maturity)



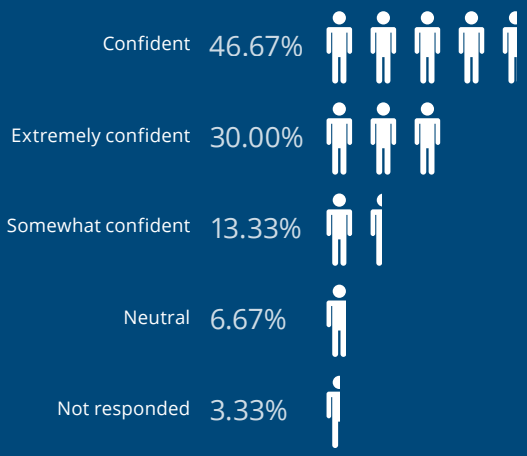
Please indicate if the following statements are true or false.

	True	False	Unsure	Not respoded
In my organisation, senior management/board of directors take an active interest in AML issues by discussing them formally at senior management/ board meetings.	28		1	1
In my organisation, the AML programme has been identified as a strategic priority.	27	2		1
My organisation has allocated adequate funding to develop and operate our AML programme.	21	7	1	1
My organisation has an enterprise wide view of our risk exposures to potential money laundering.	26	2	1	1

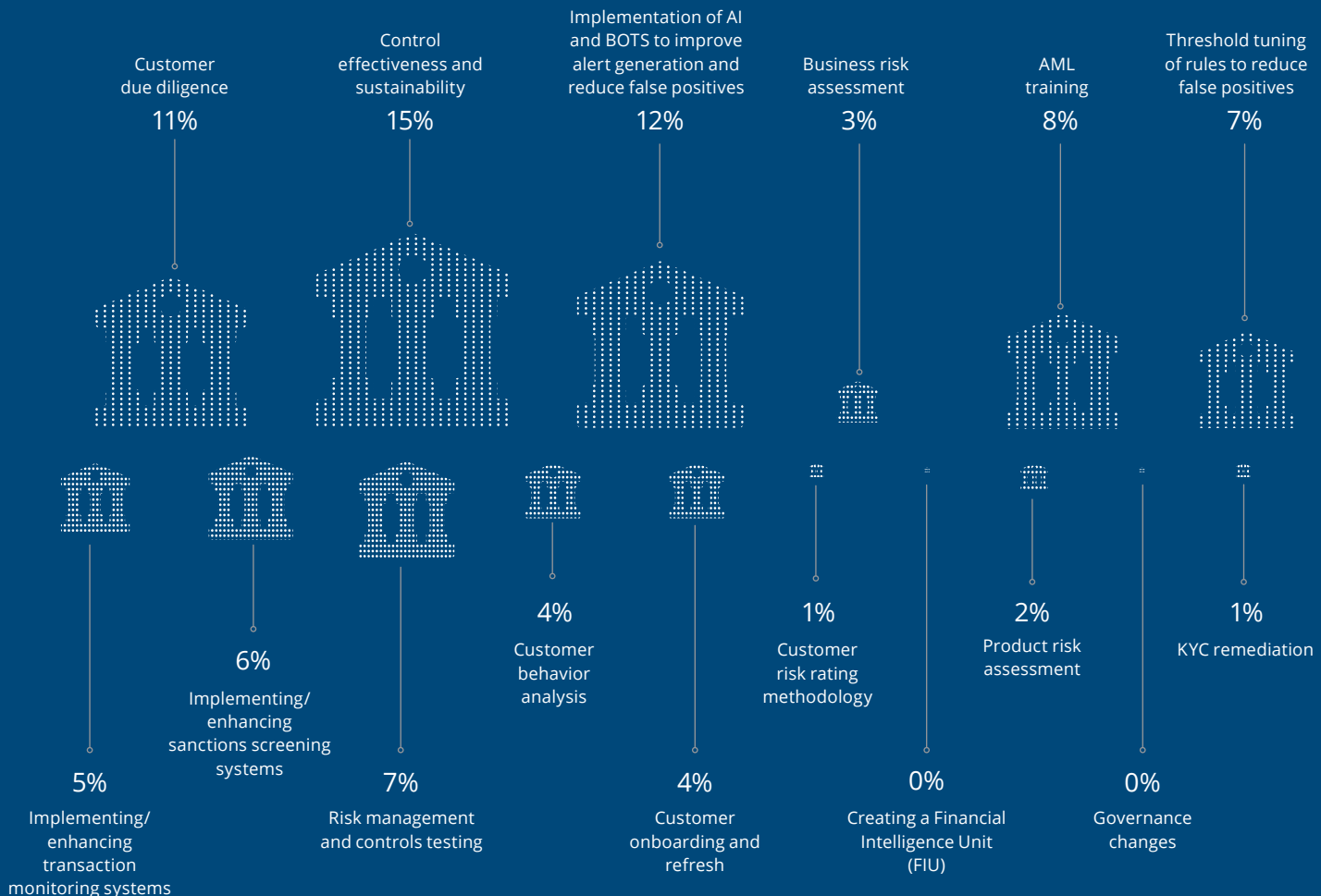
How does your group address your risk exposure to money laundering? Please select all options that apply.



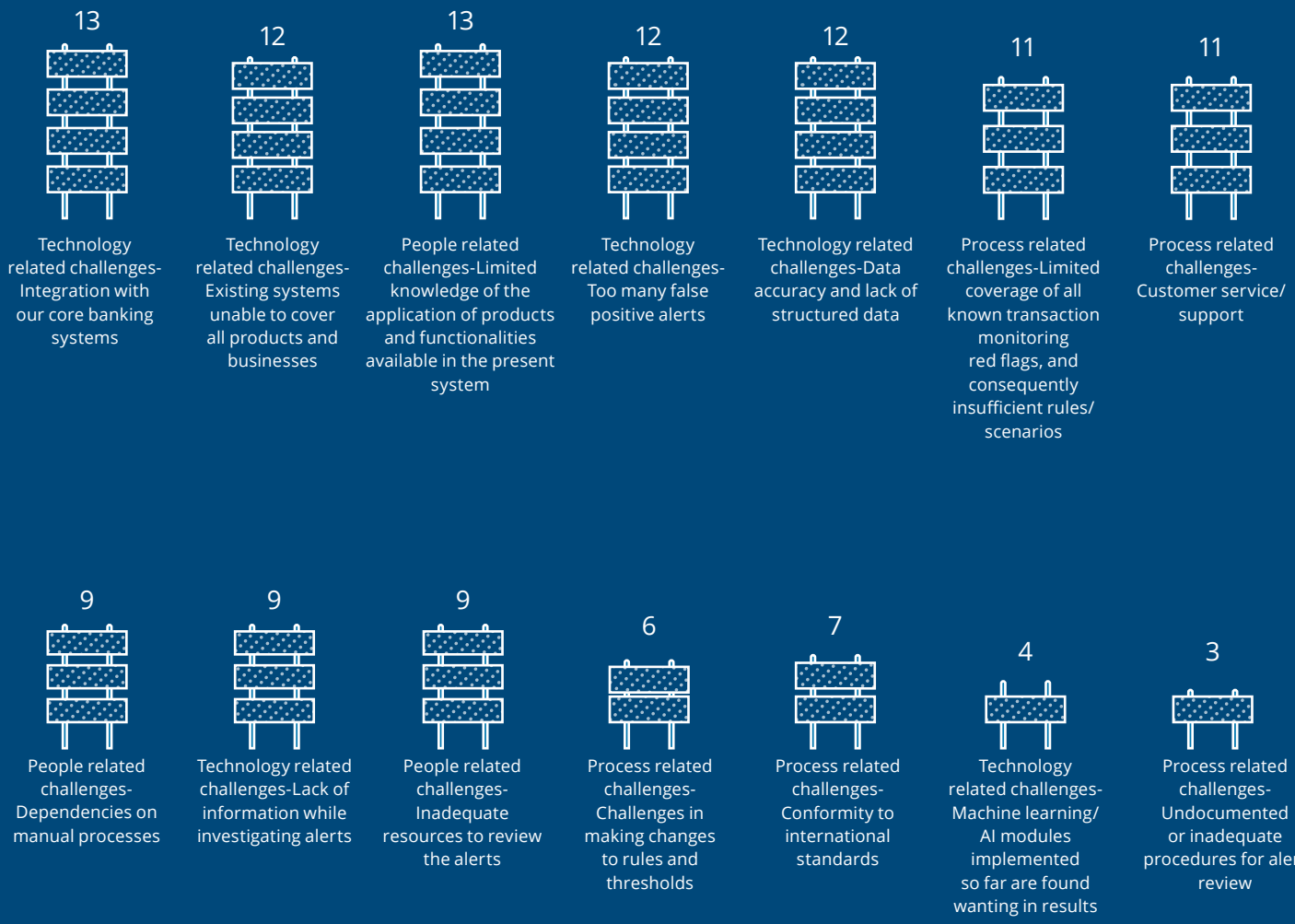
How confident are you that your financial crimes prevention/framework is compliant with all regulatory requirements and expectations?



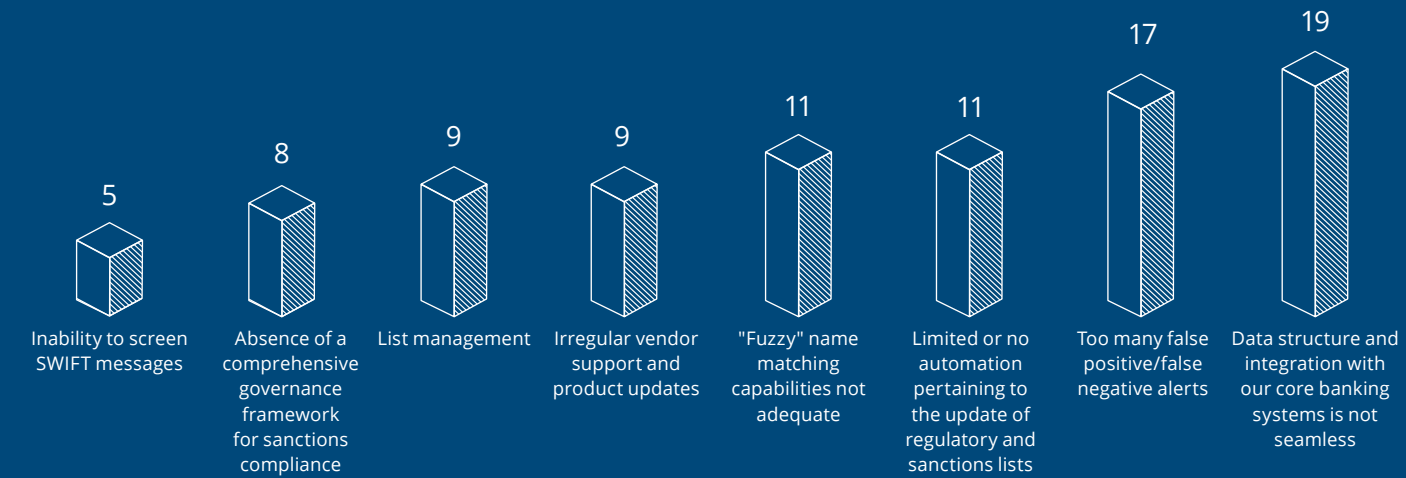
Where do you believe banks need to focus for better AML compliance in the next two years? Select the top three options that apply.



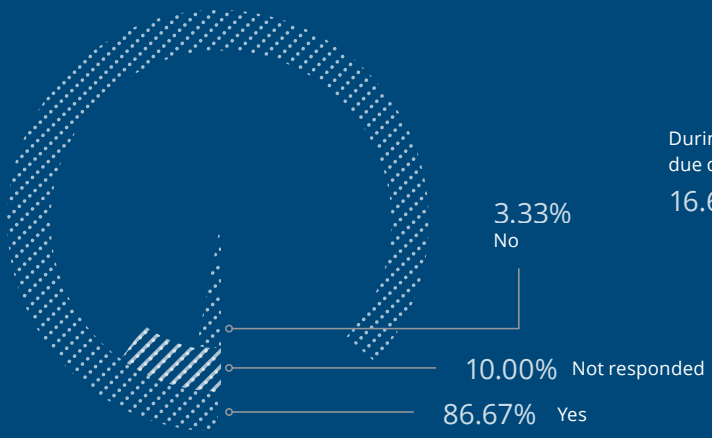
What are the biggest challenges with your current transaction monitoring system? Identify the top five challenges across all categories.



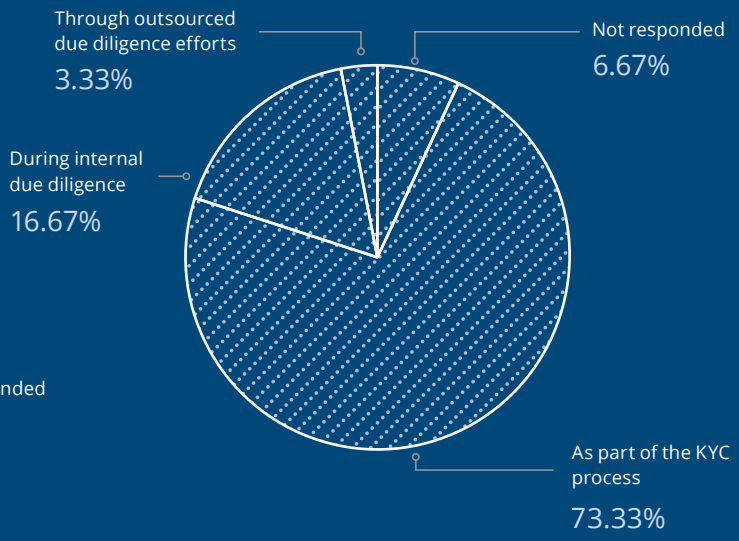
What are the factors that are affecting your confidence in your current screening solution? Tick all that apply.



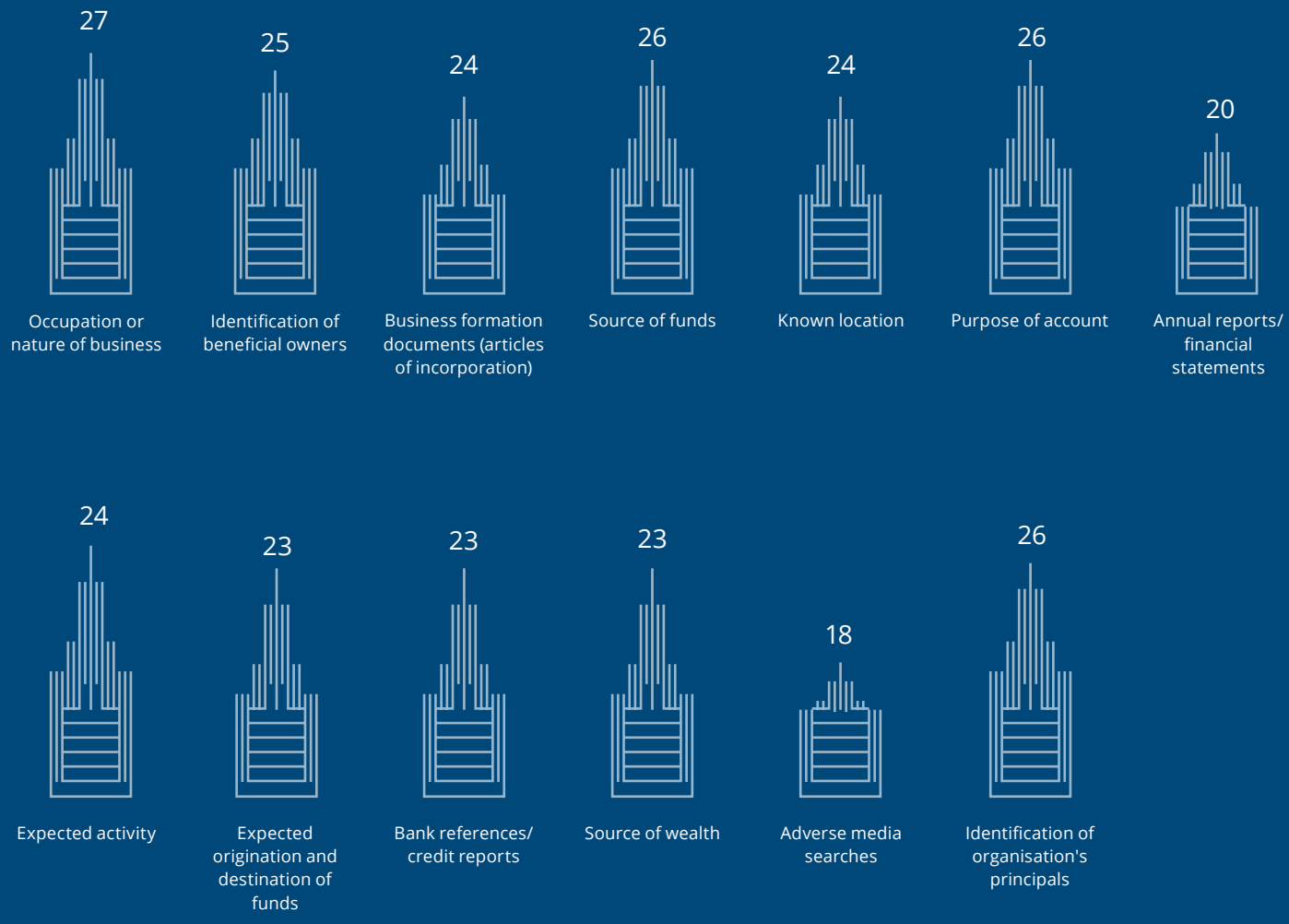
As part of the name screening process, do you also screen for politically exposed persons (PEPs)?



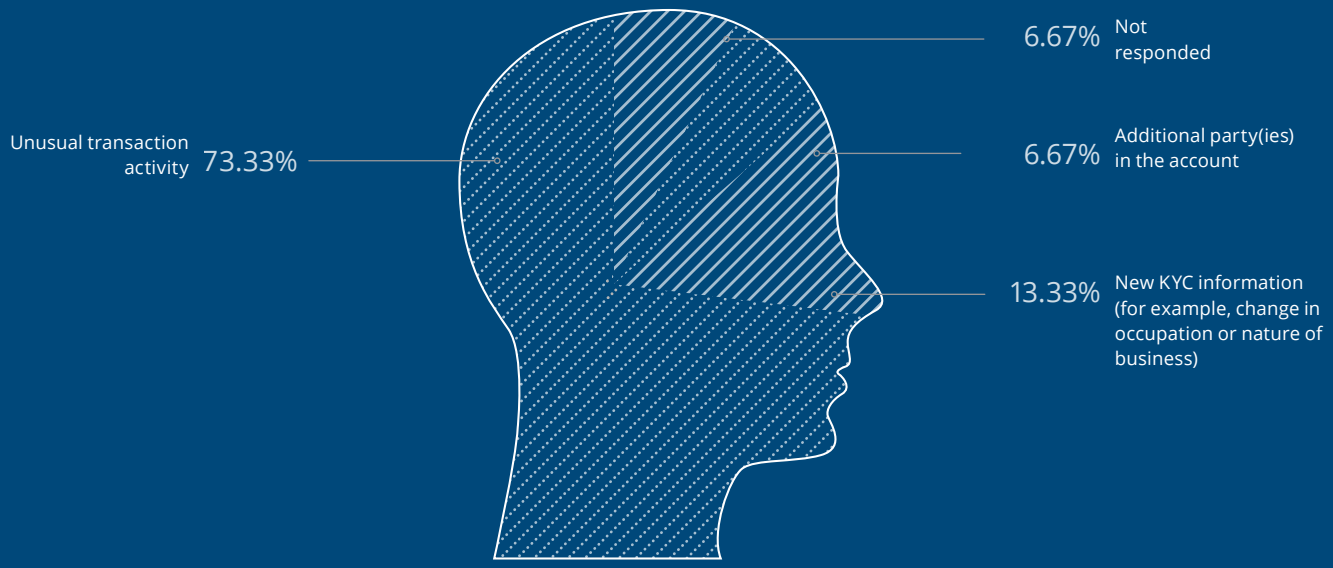
How is beneficial ownership verified in your organisation?



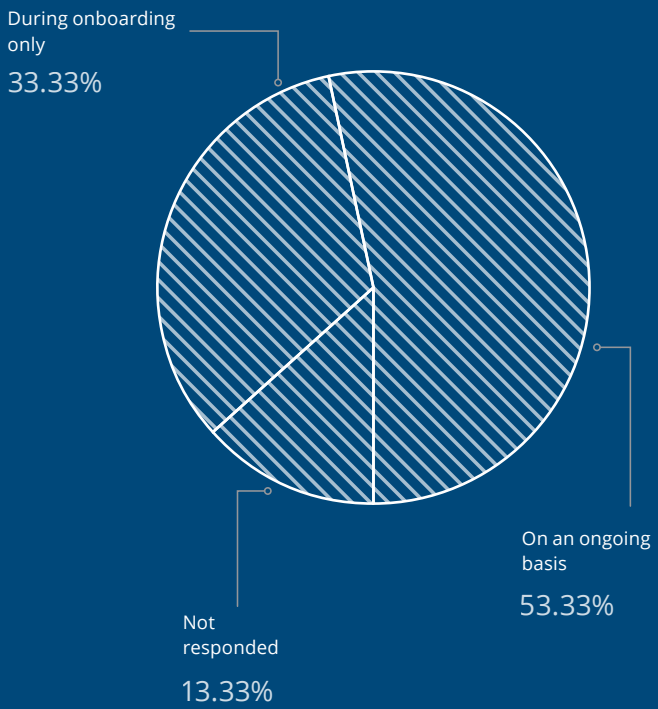
Which of the following types of information does your organisation currently gather as part of its CDD process? Tick all that apply



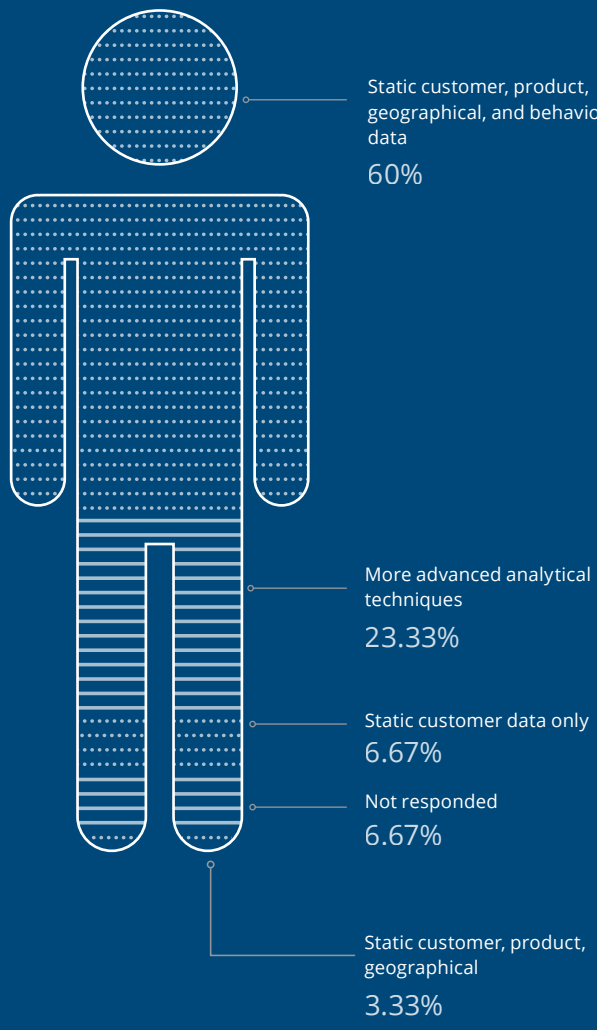
In your view, what would trigger a review or update?



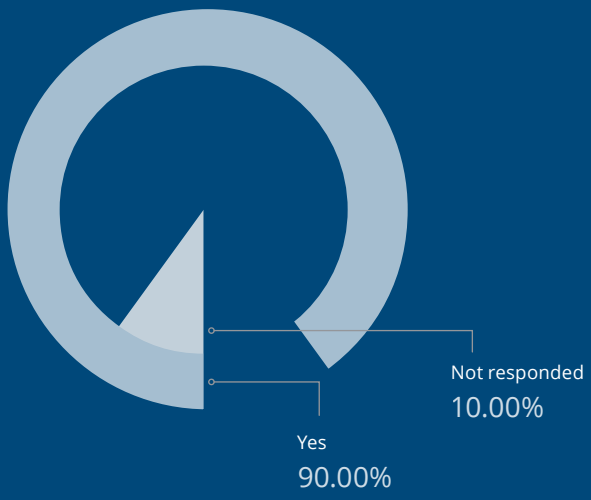
When are adverse media searches performed?



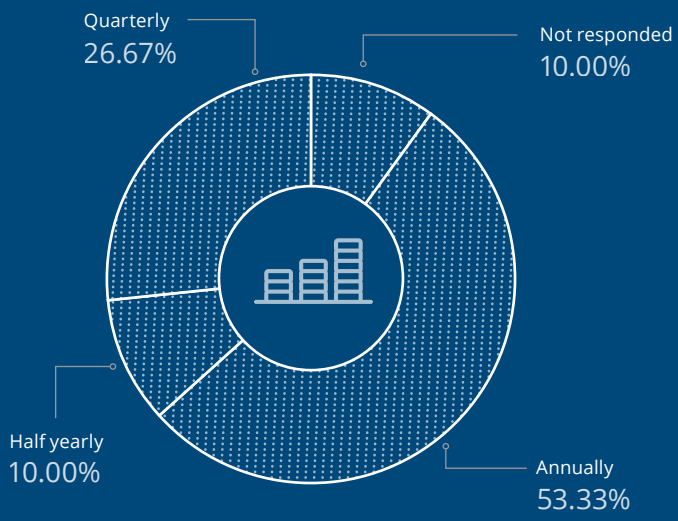
What factors are incorporated in your customer risk rating algorithm?



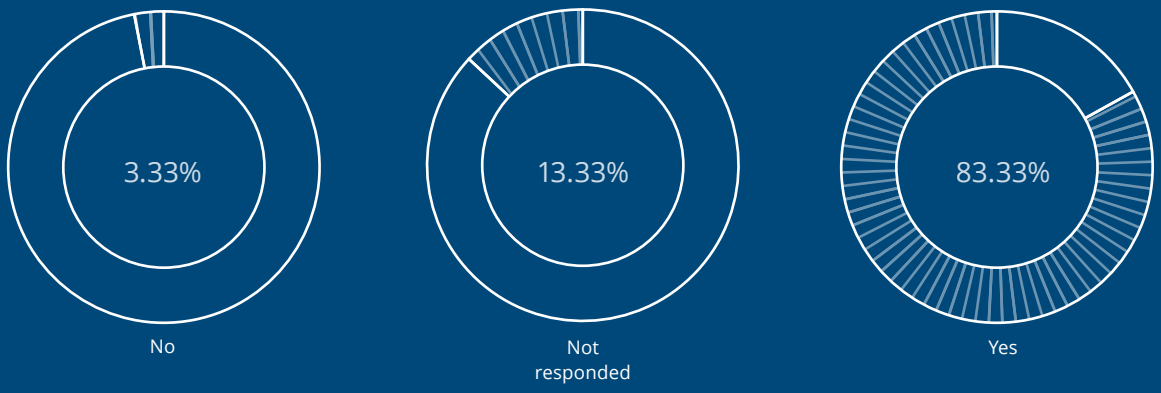
Is a tailored training on AML risks provided to your trade finance teams?



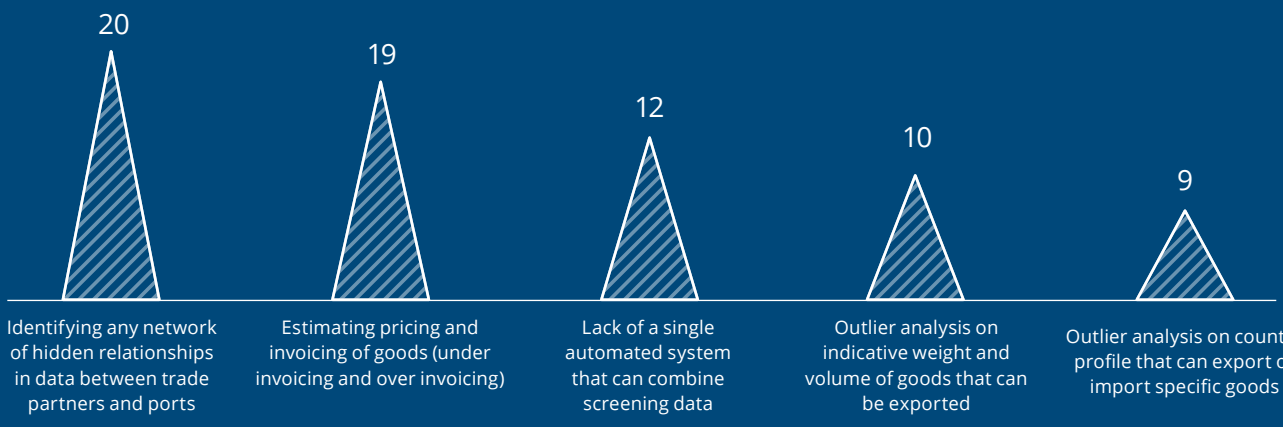
How often are risk assessments undertaken in your trade finance business?



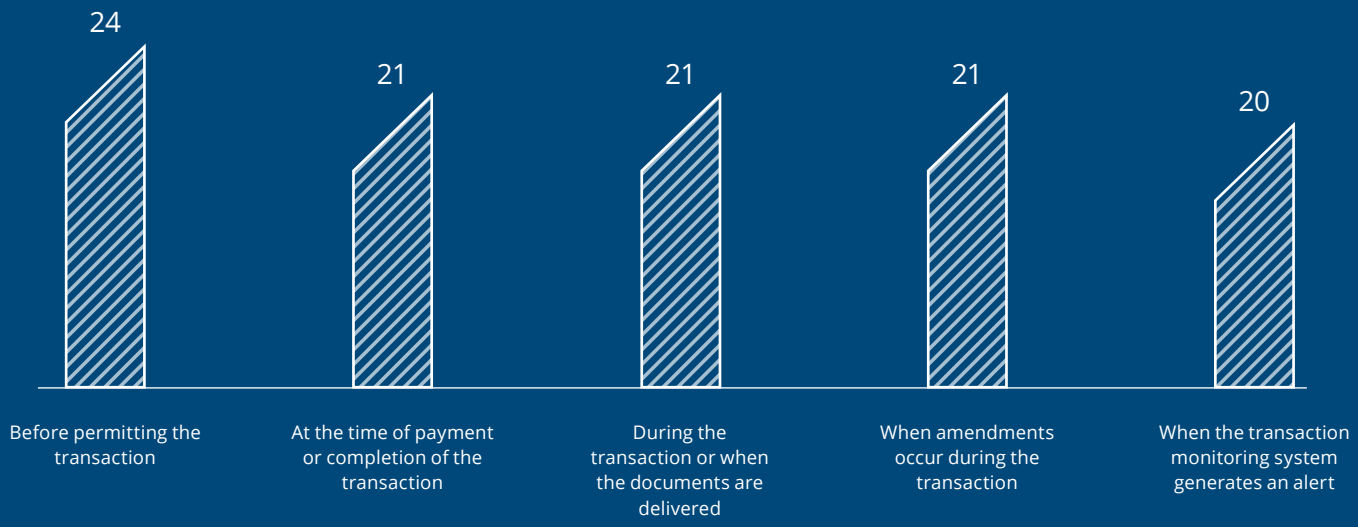
Are trade finance transactions screened against your internal, regulatory (prohibited goods), and sanctions lists?



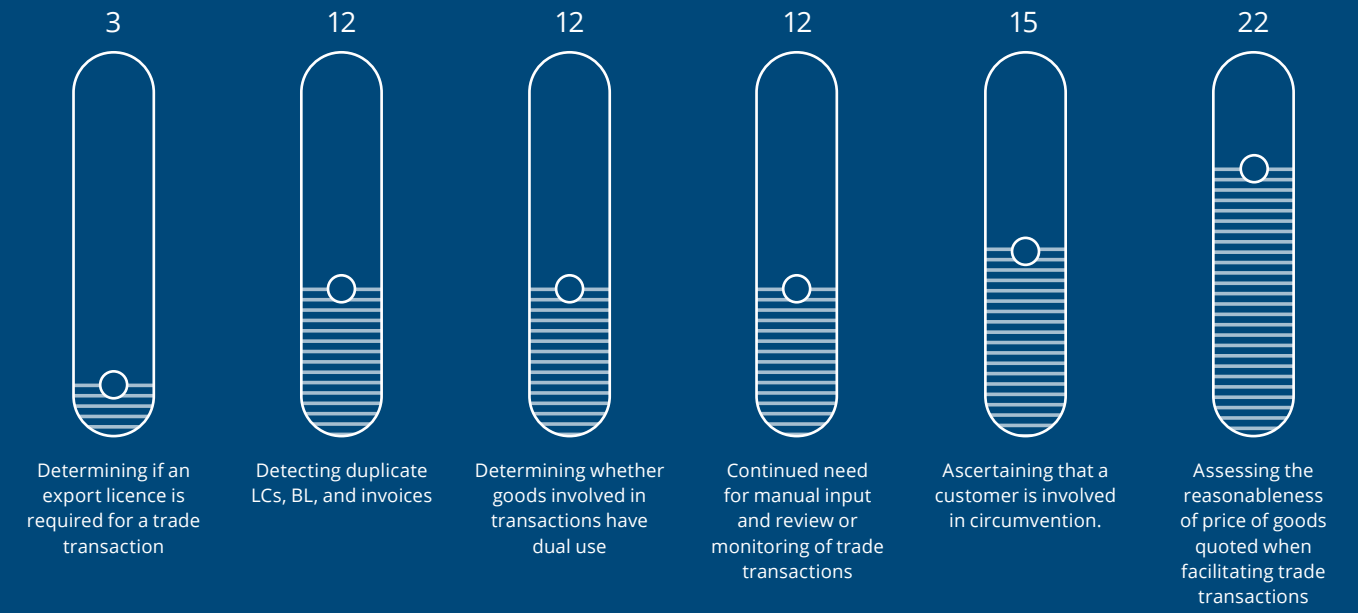
As part of processing trade finance or trade-based transactions, which of the following areas have you experienced challenges? Please tick all options that apply.



At what stages do you screen your trade finance transactions? Please select all that apply.

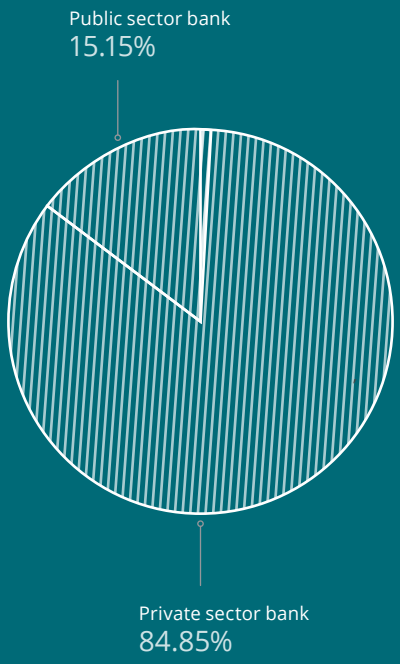


What are your biggest challenges faced while detecting TBML red flags? Select the top three options that apply.

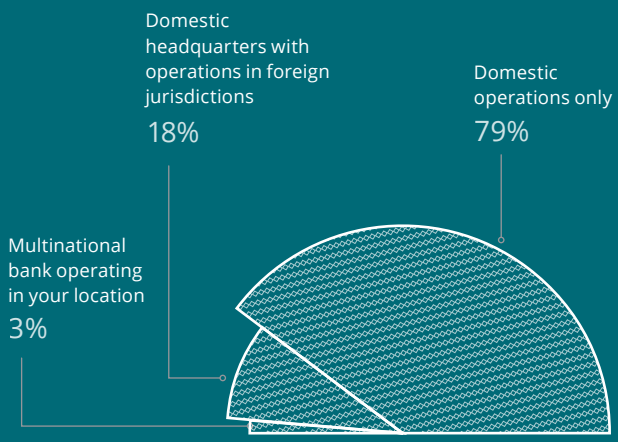


Bangladesh charts

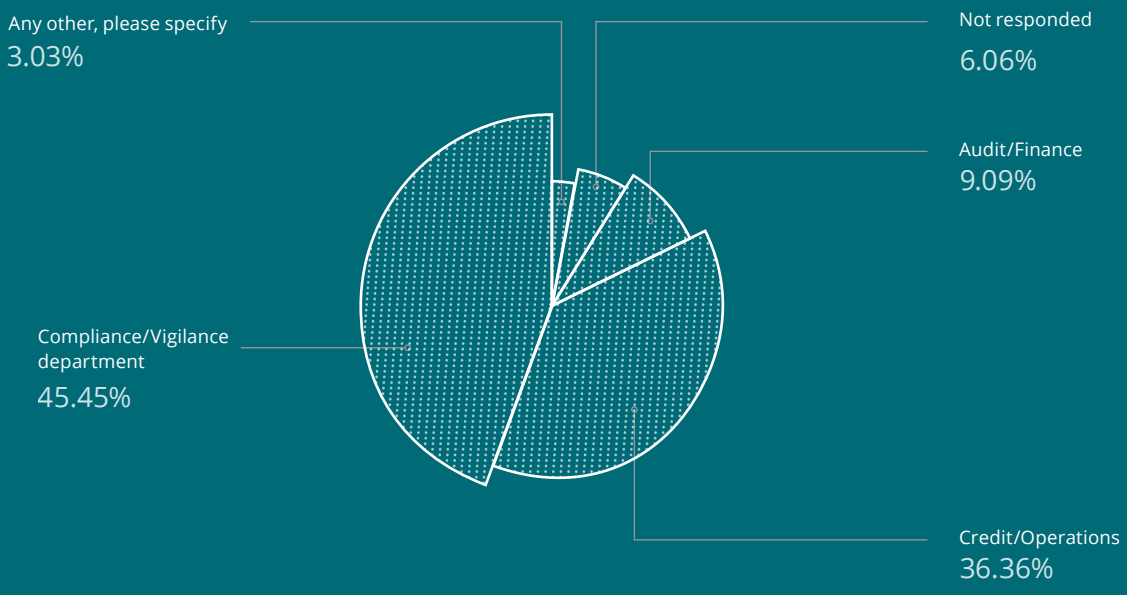
What is the type of bank you are representing?



What is the scope of your bank's operations?

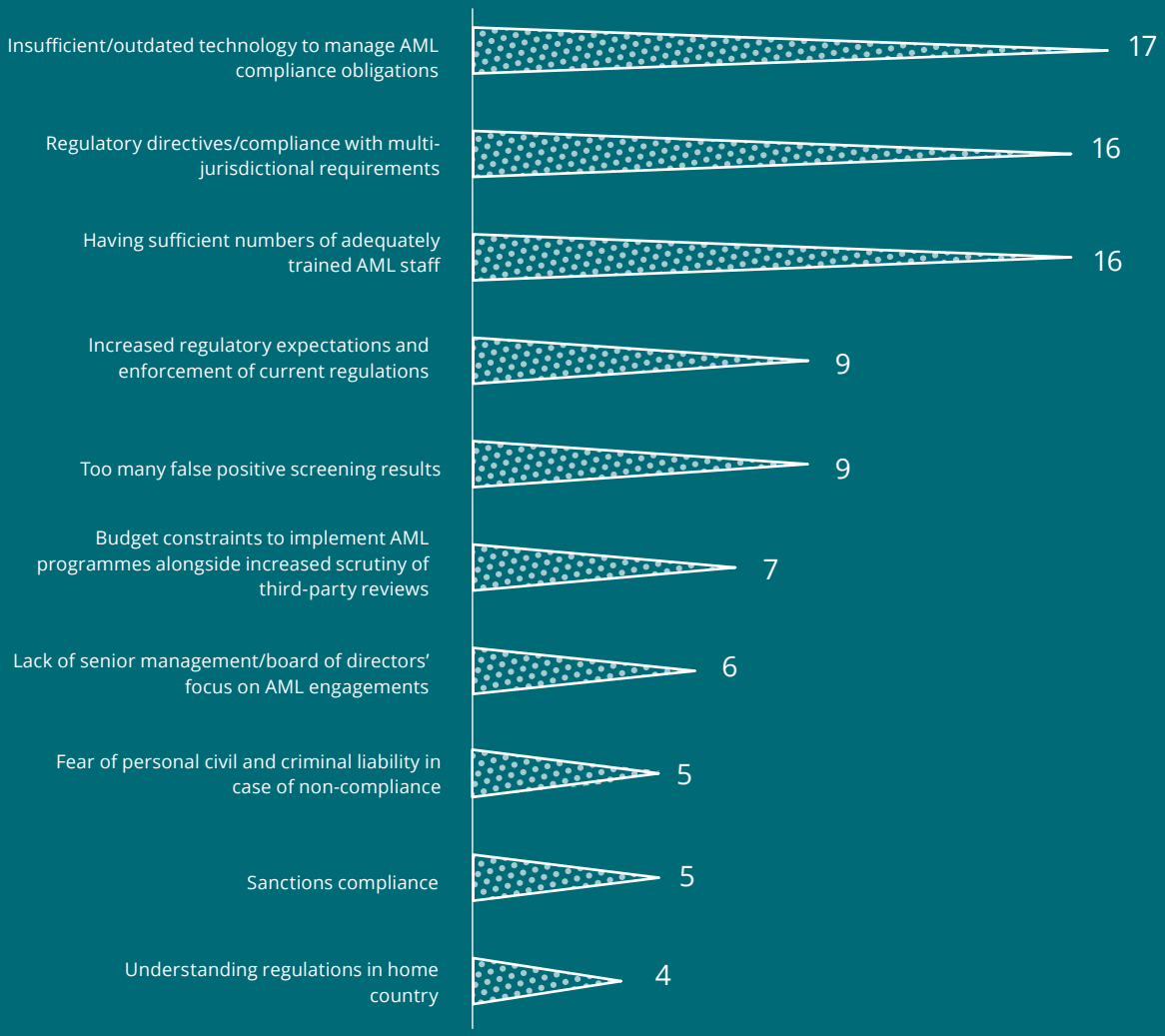


Which department do you belong to within your bank?



For multiple choice questions the total of responses will not add upto 100%

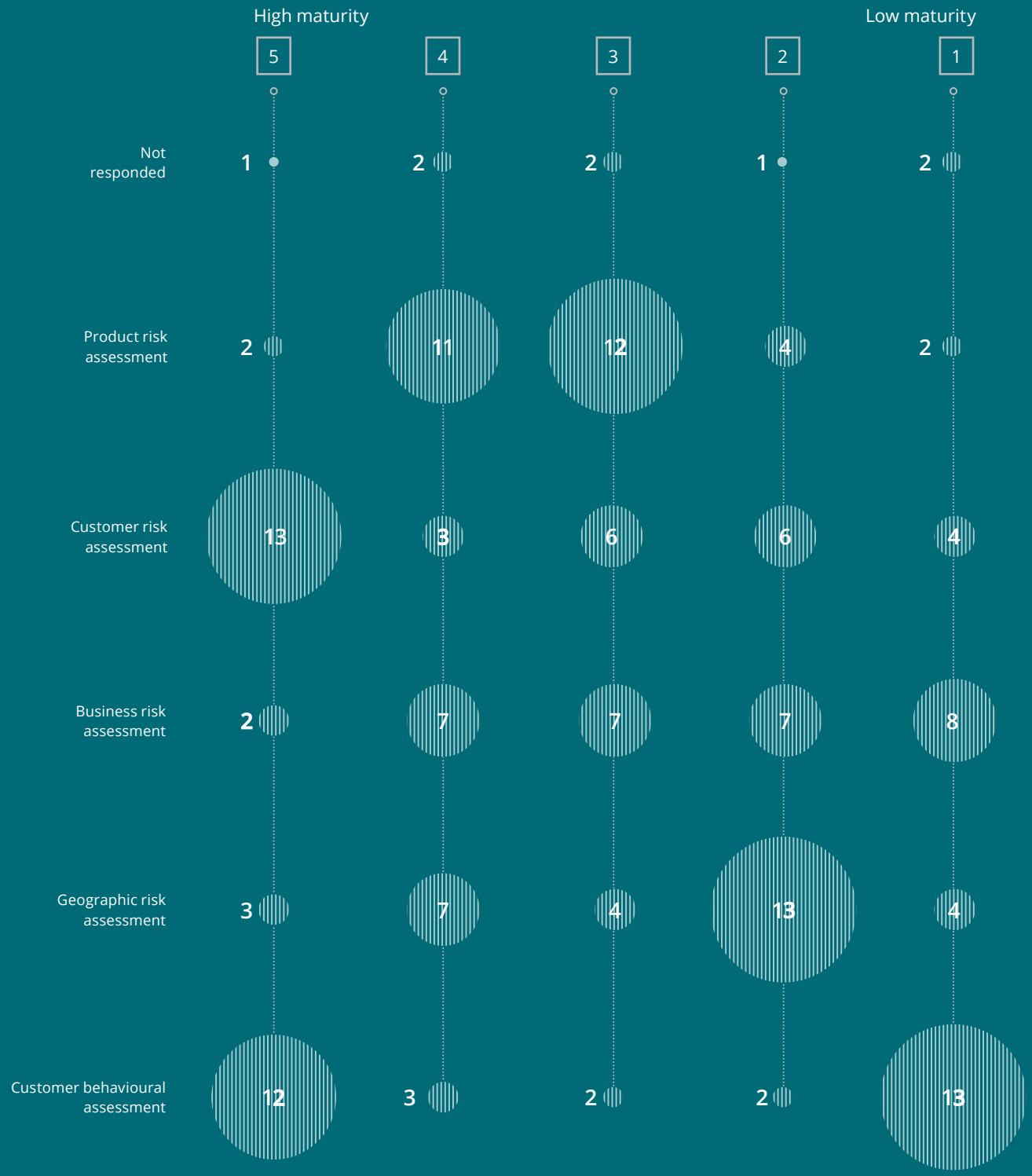
According to you, what are the biggest AML compliance challenges that banks face currently? Select the top three options.



Of the below list, please indicate which measures you have in place to manage AML and sanctions compliance.

Please identify the top five operational challenges that your organisation faces in complying with AML regulations.

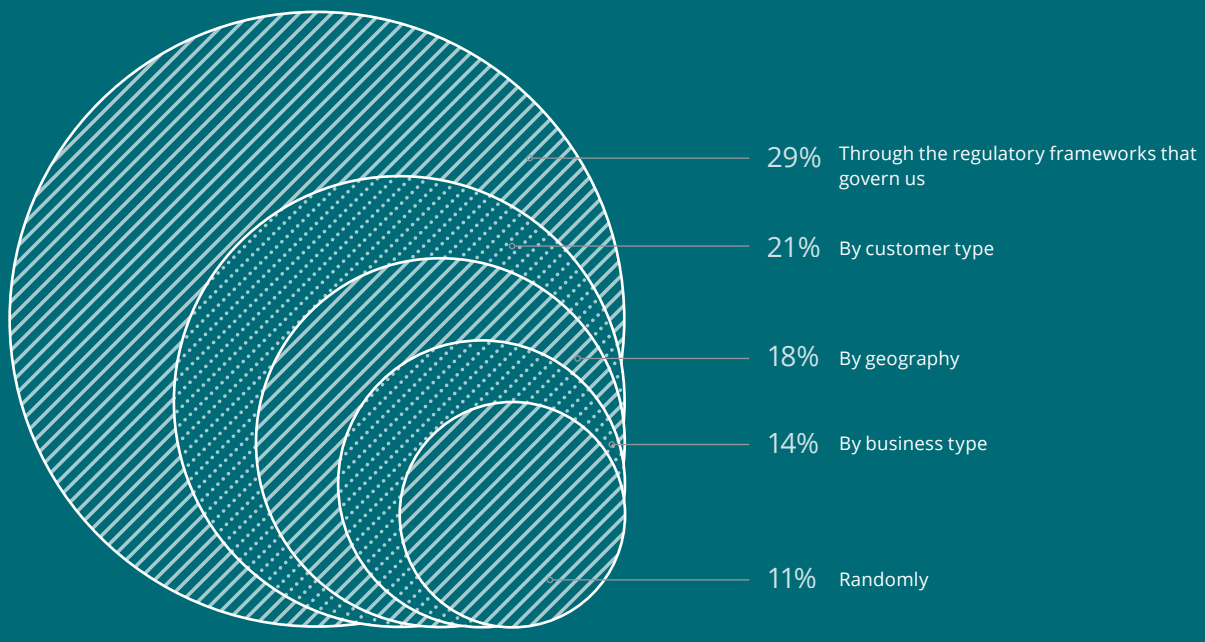
Please rate the following components of the AML programme in terms of their maturity in your organisation.



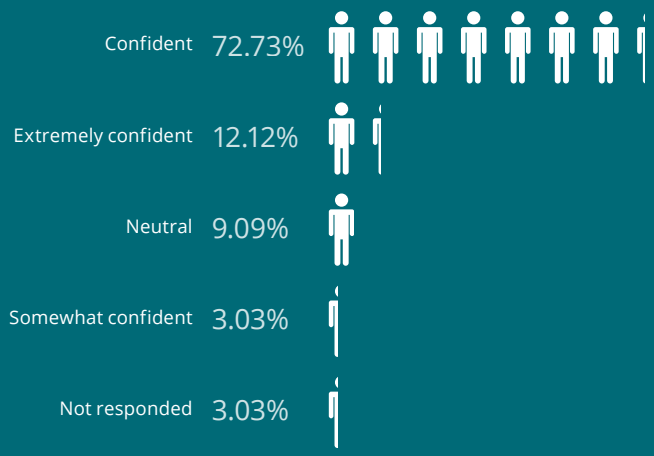
Please indicate if the following statements are true or false.

	True	False	Unsure	Not respoded
In my organisation, senior management/board of directors take an active interest in AML issues by discussing them formally at senior management/ board meetings.	27	4	1	1
In my organisation, the AML programme has been identified as a strategic priority.	30	2		1
My organisation has allocated adequate funding to develop and operate our AML programme.	26	3	3	1
My organisation has an enterprise-wide view of our risk exposures to potential money laundering.	28	3	1	1

How does your group address your risk exposure to money laundering? Please select all options that apply.

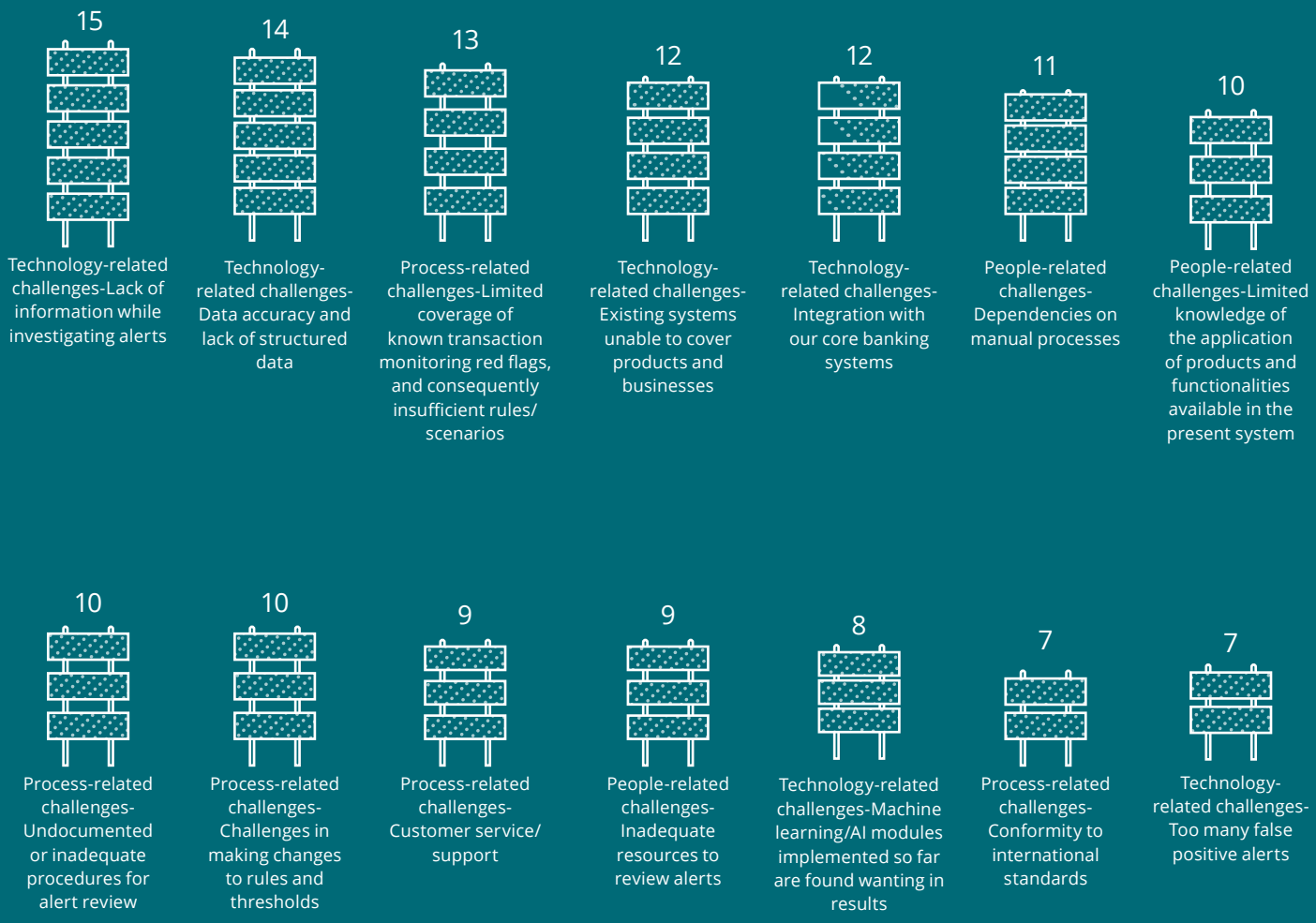


How confident are you that your financial crimes prevention/framework is compliant with regulatory requirements and expectations?

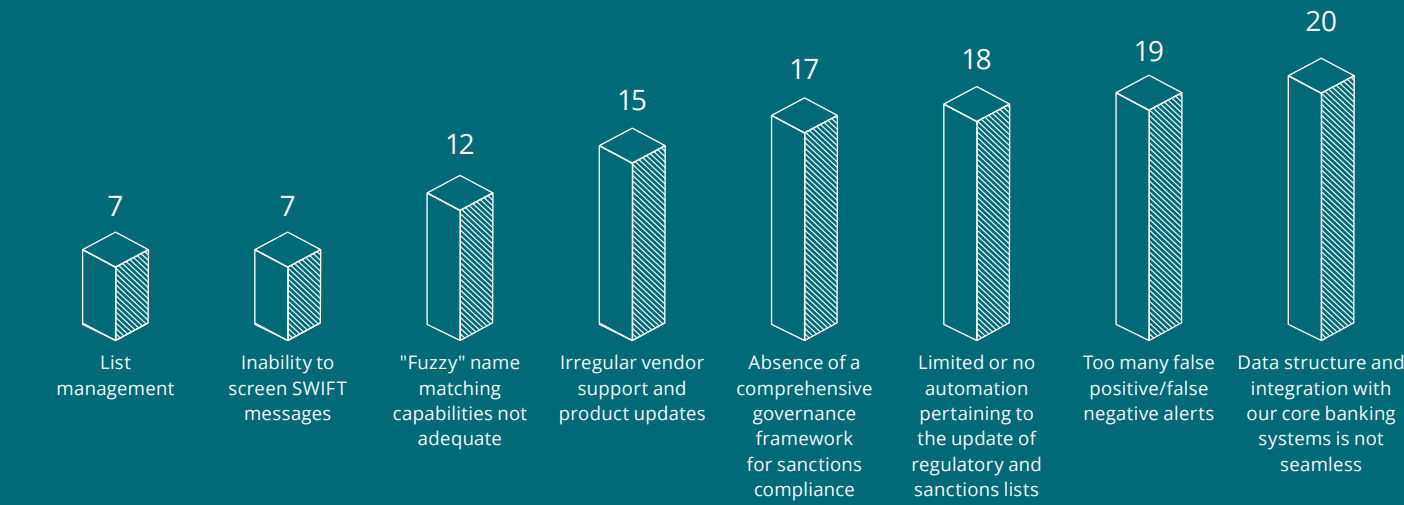


Where do you believe banks need to focus for better AML compliance in next two years? Select the top three options that apply.

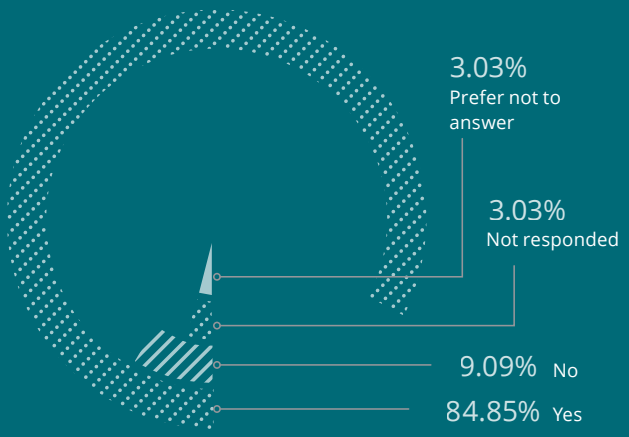
What are the biggest challenges with your current transaction monitoring system? Identify the top five challenges across categories



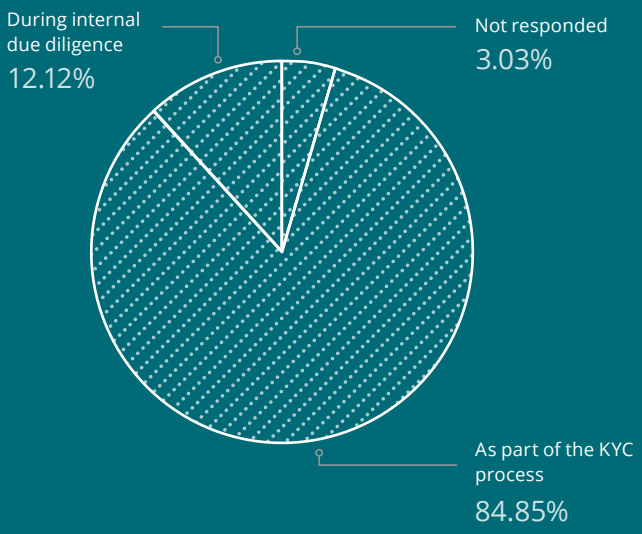
What are the factors that are affecting your confidence in your current screening solution? Tick all options that apply.



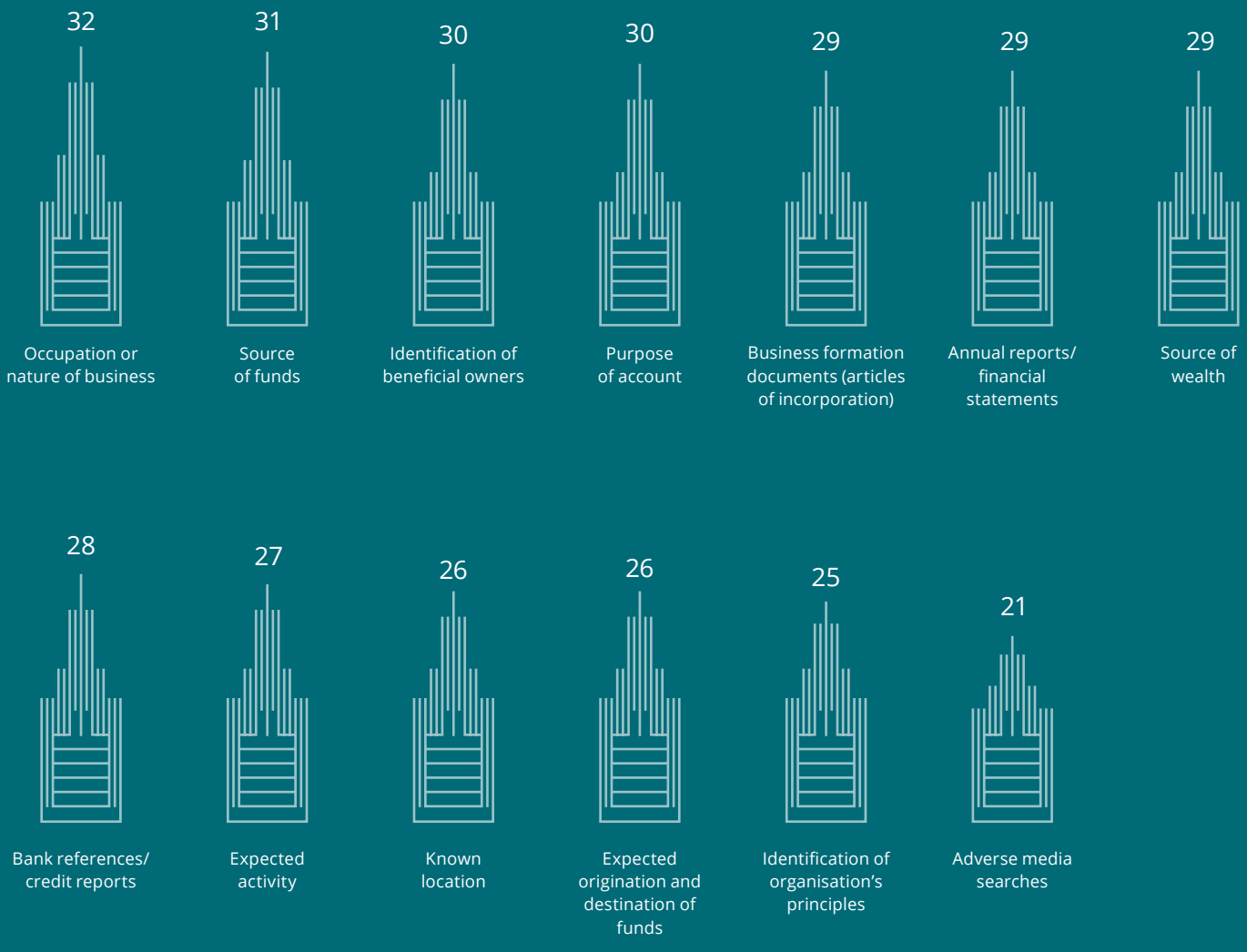
As part of the name screening process, do you also screen for politically exposed persons (PEPs)?



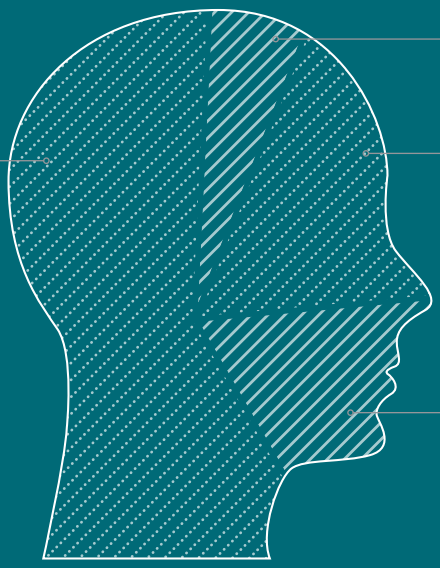
How is beneficial ownership verified in your organisation?



Which of the following types of information does your organisation currently gather as part of its customer due diligence process? Tick all options that apply.



In your view, what would trigger a review or update?



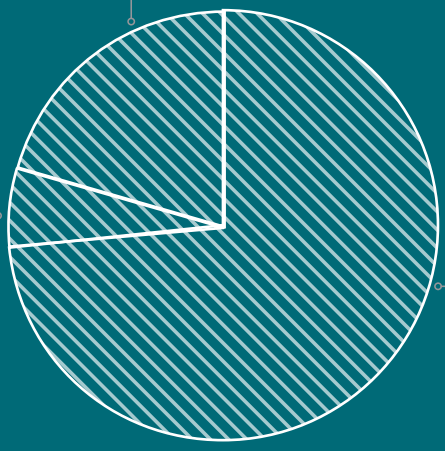
Unusual transaction activity 60.61%

3.03% Not responded

18.18% Additional party(ies) in the account

18.18% New KYC information (for example, change in occupation or nature of business)

When are adverse media searches performed?

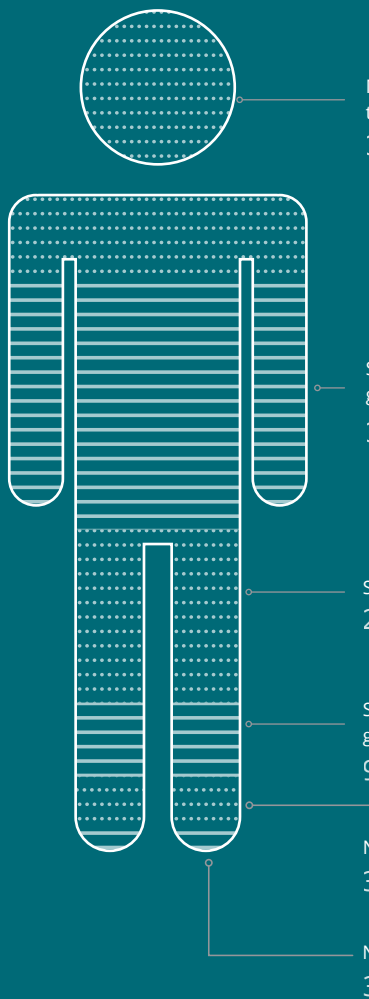


During onboarding only
21.21%

Not responded
3.03%

On an ongoing basis
75.76%

What factors are incorporated in your customer risk rating algorithm?



More advanced analytical techniques
33.33%

Static customer, product, geographical, and behavioural data
30.30%

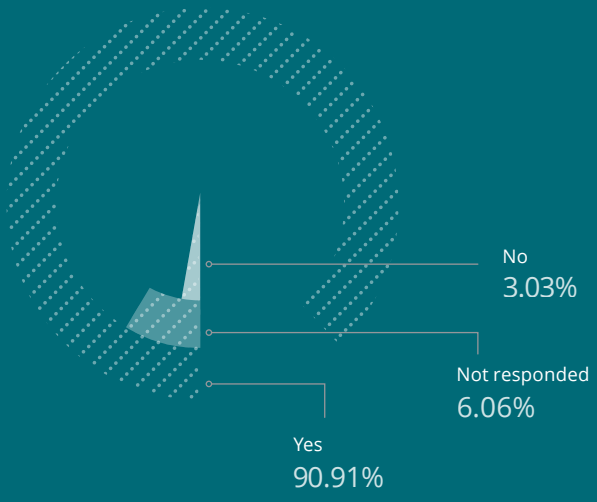
Static customer data only
21.21%

Static customer, product, geographical
9.09%

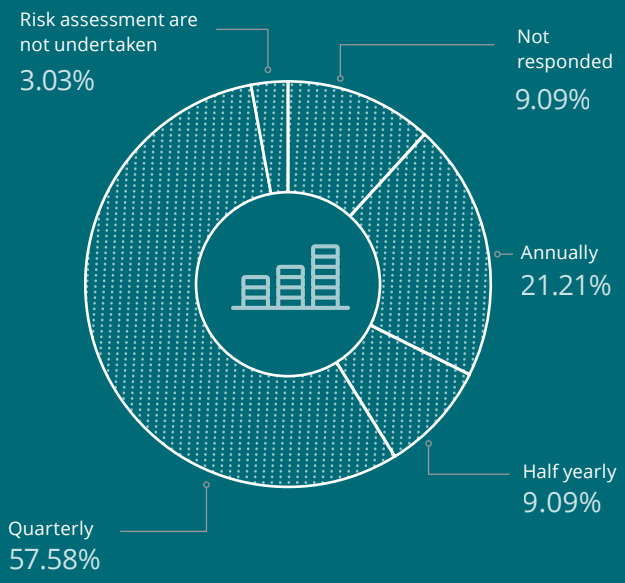
Not responded
3.03%

None of the above
3.03%

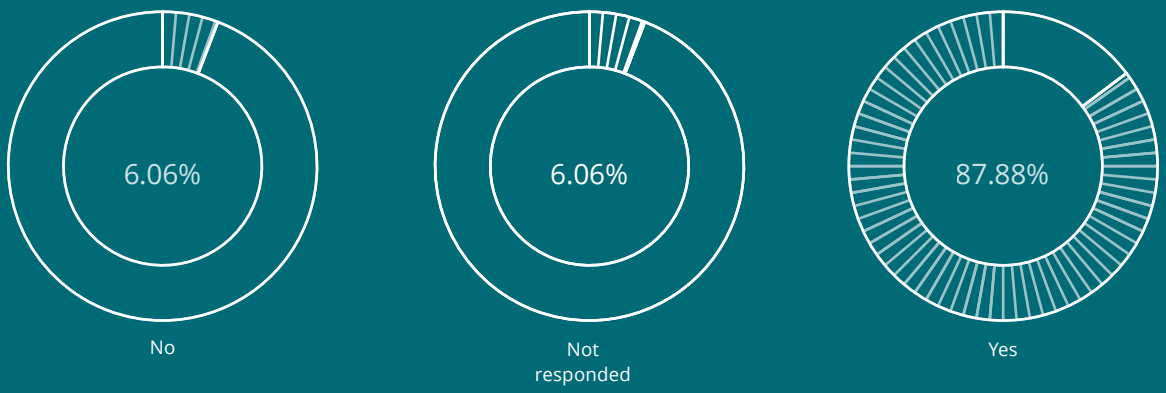
Is a tailored training on AML risks provided to your trade finance teams?



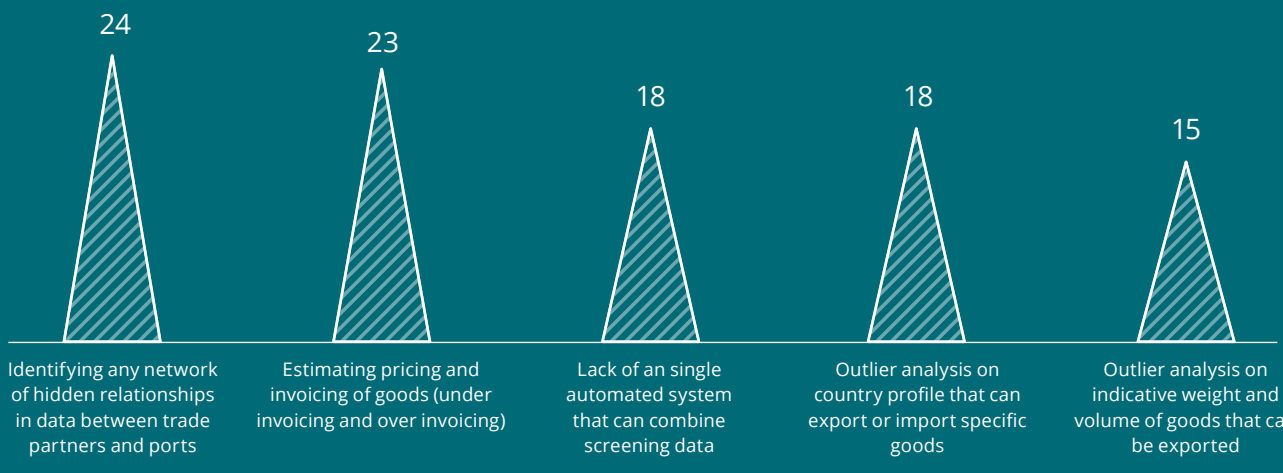
How often are risk assessments undertaken in your trade finance business?



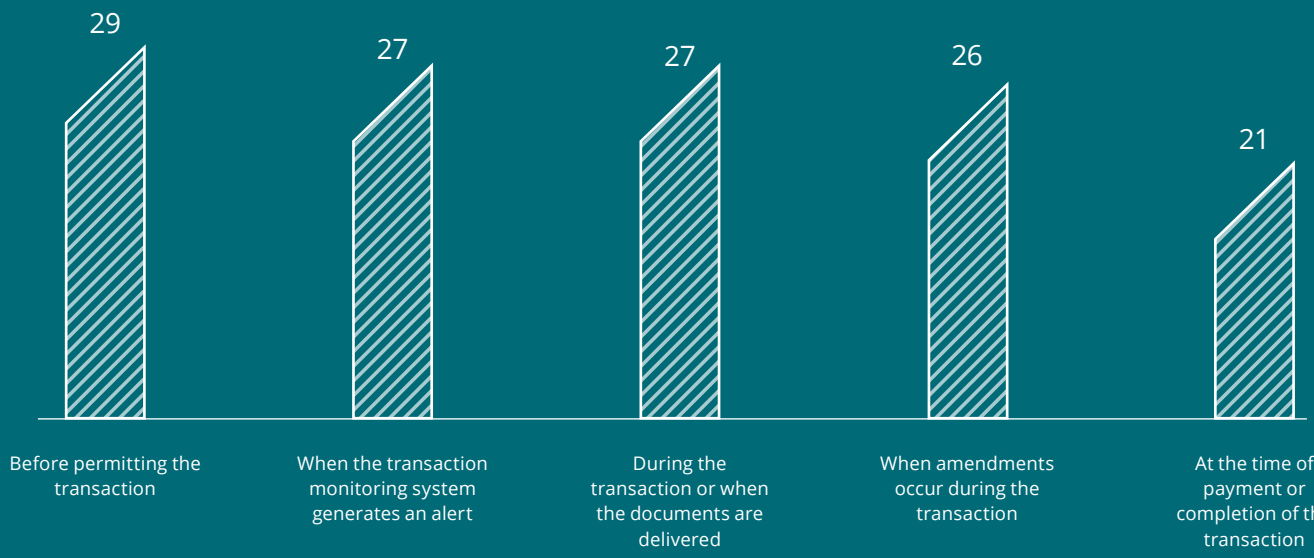
Are trade finance transactions screened against your internal, regulatory (prohibited goods), and sanctions lists?



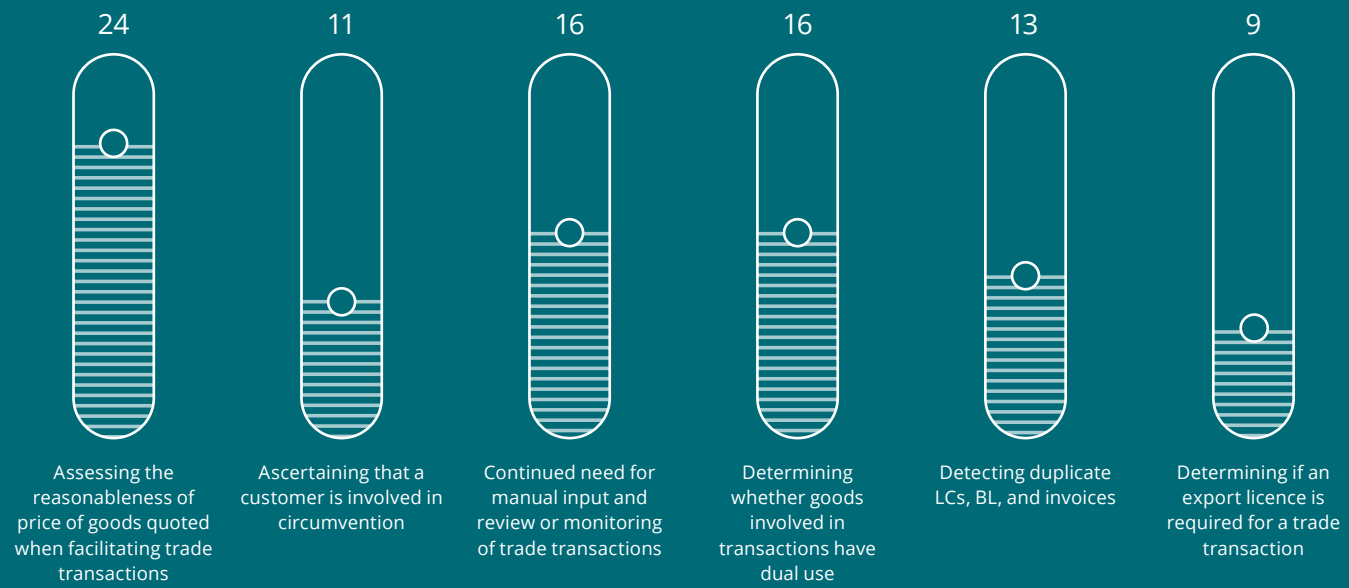
As part of processing trade finance or trade-based transactions, in which of the following areas have you experienced challenges? Please tick all options that apply.



At what stages, do you screen your trade finance transactions? Please select all options that apply.



What are your biggest challenges when it comes to detecting TBML red flags?
Select the top three options that apply.



Contacts

Nikhil Bedi
Partner and Leader - Forensic
nikhilbedi@deloitte.com

KV Karthik
Partner
kvkarthik@deloitte.com

Nishkam Ojha
Partner
nojha@deloitte.com

Deloitte.