

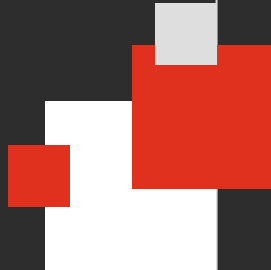
PwC 2023 AML Survey Results

December 2023



Contents

01	Introduction	03
02	AML Survey results	06
—	Part 1 Results: Governance	07
—	Part 2 Results: Customer Due Diligence (CDD)	14
—	Part 3 Results: AML / CFT Business Wide Risk Assessment (BWRA)	22
—	Part 4 Results: Technology Analysis	28
—	Part 5 Results: Management Information	34
03	Key actions businesses can take today	38



01

Introduction





Introduction

PwC carried out a survey amongst regulated Irish financial services firms in Summer 2023 covering a wide range of industries, including funds, banking, e-money, payment services and insurance firms. The aim of the survey was to identify the extent of challenges and opportunities for regulated financial services firms in the management, identification and oversight of anti-money laundering and financing terrorism in the light of a new regulation and increased supervision coming in 2024.

AML/CFT continues to be a key focus for regulators in Ireland and across Europe. This means that compliance with AML/CFT controls in regulated entities in Ireland remains a top priority for Senior Management and the Board. Implementing a robust AML/CFT framework can be challenging due to the pace of change from a regulatory perspective but also due to the ways in which criminals are adapting and evolving their methods of ML/FT to evade established controls in place within regulated financial services entities.

In addition to this, there is also significant change coming down the line from a regulatory perspective with the establishment of the new EU AML Authority (AMLA), as well as the introduction of a new directly applicable regulation. These changes fall under the EU's AML Package, which was originally presented by the European Commission in July 2021.

“Ireland continues to progress in strengthening measures to tackle money laundering and terrorist financing and has received an increased rating in the most recent inspection by the global Financial Actions Task Force in 2022”.

“Technology is the only way to keep up with the race against financial crime and there is much more to do on automation. Many clients have invested over the years but the key to success is a fully integrated technology system. Disparate technology makes it more difficult to gather information, identify suspicious activity and report financial crime.”

Sinead Ovenden
Financial Service Regulatory Partner
sinead.m.ovenden@pwc.com

Introduction

The 2023 AML/CFT survey focused on

- Identifying how AML operating models are evolving and adapting across the financial services industry in Ireland;
- Comparing and contrasting how various entities across the Financial Services industry manage compliance with AML legislation and guidance;
- Capturing emerging trends and opportunities for automation of AML/CFT activities. *

Responses to the survey were received from a wide range of financial services entities with the results analysed and grouped into the following sectors:

- Banking Industry
- Asset & Wealth Management (AWM) Industry
- E-Money & Payment (EMI/PI) Industry
- Insurance Industry
- Other industries (Credit unions, Credit servicing, Brokers / Retail Intermediaries, schedule 2 activities)



02

AML Survey results





Part 1 Results

Governance



AML Survey results

Part 1 results: Governance

The CBI AML/CFT Guidelines note that “insufficient or absent AML/CFT risk management, governance, policies, controls and procedures exposes firms to significant risks, including not only financial but also reputational, operational and compliance risks”. The CBI expects ML/TF risk management measures to be adopted by firms on a risk-based and proportionate basis, informed by the firm's Business Risk Assessment and in compliance with the CJA 2010.

To achieve good governance and compliance, AML/CFT roles and responsibilities should be clearly defined and documented. The traditional method within regulated firms of overseeing and ensuring compliance is through a “**three lines of defence**” model. With this model, AML/CFT risks are owned and managed directly by the first line of defence, the second line of defence oversees the first line and the third line of defence provides independent assurance of the first and second line.

Alongside the three lines of defence model, the Board should be able to demonstrate effective governance and oversight of the Firm's AML/CFT compliance framework at a minimum through:



The review and approval of the Business Risk Assessment on at least an annual basis, as well as the methodology used by the firm;



The review and approval of the firm's AML/CFT Policies and Procedures, as well as material updates to same;



Ensuring that appropriate reporting lines are in place which facilitate the escalation of AML/CFT issues from Compliance for discussion by the Board;



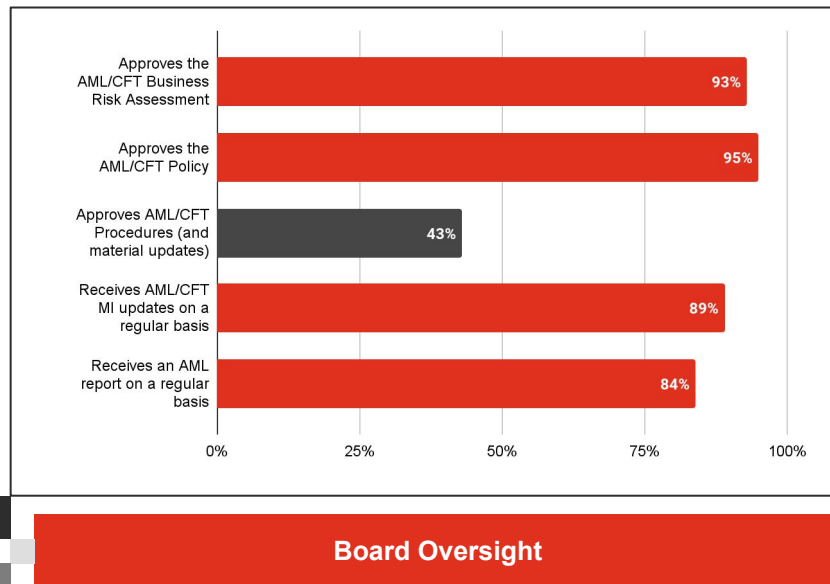
Ensuring that AML/CFT appears as an agenda item at regular Board meetings and that discussions and outcomes are reflected in the minutes (an annual compliance officer / MLRO report should also be presented to the Board).



Ensuring that the firm's AML/CFT function is adequately resourced and that reviews are regularly undertaken to ensure not only appropriate numbers but also the correct skill set, as well as appropriate access to systems and resources.

AML Survey results

Part 1 results: Governance



Employee breakdown - first and second line AML/CFT activities

The number of employees staffed within an AML function will be dependent on a variety of factors, including the size of the organisation, the number of customers and also the AML/CFT risk profile of the organisation. While trends are displayed through the results of our survey, these need to be considered alongside the fact that results can vary depending on individual firms size and needs.

Overall, the majority of firms (43% of respondents) have **between 2 - 10 employees responsible for AML/CFT activities in their first line of defence**, with 18% of firms confirming that they have between 11 - 50 employees responsible for AML/CFT activities in their first line of defence. The main outlier here is Credit Institutions, where 60% of respondents noted that they have > 50 employees in their first line of defence responsible for AML/CFT activities. This result aligns with the fact that the majority of Credit Institutions confirmed that they fall under the definition of a “large firm” and also that they manage > 5,000 new customers on a monthly basis.

Similarly, the majority of firms (52% of respondents) have **between 2 - 10 employees responsible for AML/CFT activities in their second line of defence**, with this response slightly higher for respondents from EMI/PI firms (60% of respondents) and Insurance firms (80% of respondents). The majority of respondents from Credit Institutions (60%) confirmed that they have between 11 - 50 employees responsible for AML/CFT activities with their second line of defence.

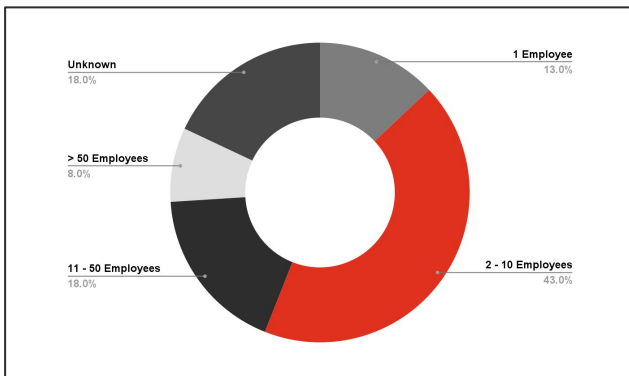
AML Survey results

Part 1 results: Governance

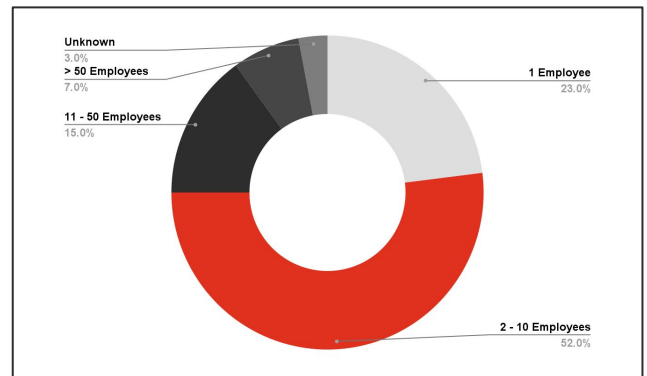
Employee breakdown- first and second line AML/CFT activities

Interestingly, 20% of respondents from EMI/PI firms noted that they have > 50 employees responsible for AML/CFT activities within their second line of defence. It is possible that AML Operational activities, such as KYC and Transaction Monitoring remain the responsibility of the second line of defence within these firms. There is no guidance which dictates where these activities must sit, however, we are seeing clients moving these types of operational AML/CFT activities from the second line to the first line.

While there are no specific regulatory requirements in how firms set up their business model to manage AML/CFT risks, the CBI Guidelines note that where the three lines of defence model is used, there should be **adequate and effective coordination** between the front line business unit, risk, compliance and internal audit, or equivalent within the Firm, to ensure robust and well-structured oversight, as well as effective coordination of resources to manage overlap in areas of review.



Employee Breakdown - 1LOD FT AML/CFT Activities



Employee Breakdown - 2LOD FT AML/CFT Activities

AML Survey results

Part 1 results: Governance

Employee breakdown- first and second line AML/CFT activities

Firms must be able to allocate clear responsibility across the three lines, it is imperative to develop some consensus around what the three lines are expected to do, for example:

First line of defence



Responsible for owning and managing AML/CFT risks.

Second line of defence



Responsible for overseeing AML/CFT risks, as well as compliance with your organisations AML/CFT framework.

Third line of defence



Provides independent assurance over relevant AML/CFT risks, processes and procedures.

AML framework

Section 30A (2) of the CJA 2010 requires regulated firms to have regard for various sources of information when documenting their Business Wide Risk Assessment. These sources include relevant information contained in the National Risk Assessment, guidance issued by the CBI, as well as guidance issued by relevant European bodies, such as the European Banking Authority (EBA). Our survey asked respondents what sources of information are used by their firms to ensure compliance with AML/CFT requirements, and unsurprisingly over 90% of respondents across all sectors confirmed that their firm considers all relevant Irish and European guidance and legislation, as well as guidance issued by FATF. An outlier here was the National Risk Assessment **where only 79% of respondents** confirmed this as a source which is considered when ensuring compliance with AML/CFT requirements.

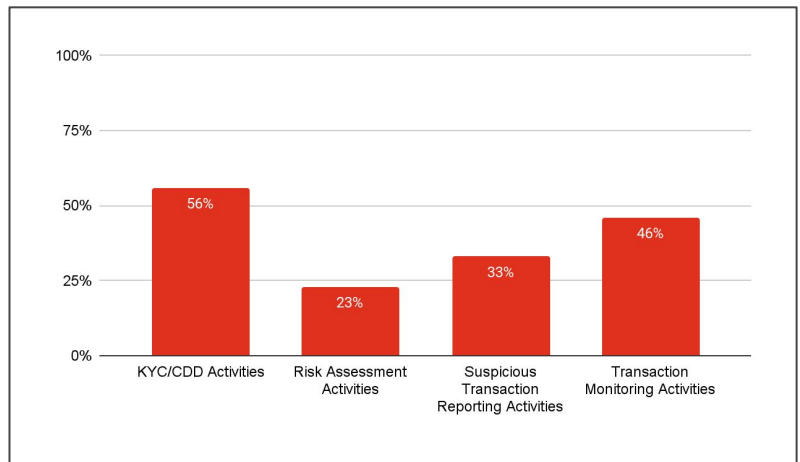
The National Risk Assessment is a valuable resource for regulated entities as it provides key insights into AML/CFT threats and vulnerabilities in various sectors in Ireland with a particular focus on the financial services sector.

AML Survey results

Part 1 results: Governance

Outsourcing of AML /CFT activity

Outsourcing of AML/CFT activities continues to remain a key tool for regulated firms in Ireland. There can be many reasons why firms outsource activities, for example, lack of internal resources, centralisation of AML/CFT activities to the group or financial efficiencies. These activities may be outsourced to Third Party Service Providers or they may be outsourced to other entities within an organisations own group of companies.



Outsourcing of AML/CFT activities

Where AML/CFT activities are outsourced, the regulated firm **remains ultimately responsible** for compliance with its obligations under the CJA 2010. The firm should ensure that there is **effective oversight and management** of the AML/CFT activities being outsourced, including a documented agreement which clearly defines the obligations of the outsourcing service provider.

61% of respondents to our survey confirmed that they outsource some/all of their AML/CFT activities. The outsourcing of AML/CFT activities is **particularly high in EMI/PI firms**, where 87% of respondents confirmed that they outsource some/all of the AML/CFT activities. This is contrasted with the AWM industry where 50% of respondents disclosed that they manage all of their AML/CFT activity internally, while 40% of respondents from Credit institutions and Insurance firms also manage all of their AML/CFT activities internally within their organisation. The higher volume of outsourced activities with EMI/PI firms may be attributed to the fact that these firms are more likely to be newer entrants to the markets and are therefore still in the process of establishing their regulated business in Ireland.

From the responses to our survey, the most popular AML/CFT activity being outsourced by regulated firms in Ireland is KYC/CDD activities, where 56% of respondents confirmed that all or elements of this activity are outsourced by their firm. This is particularly high in EMI/PI firms where 80% of firms outsource elements of this activity. Similarly a very high number of respondents (87%) from EMI/PI firms confirmed that Transaction Monitoring activities are outsourced by their firm. This is contrasted with the overall figure where 46% of all respondents confirmed that Transaction Monitoring activities are outsourced by their firm.

AML Survey results

Part 1 results: Governance

Outsourcing of AML /CFT activity

The number of firm outsourcing Suspicious Transaction Reporting and Risk Assessment activities is much lower, with 33% of respondents confirming that Suspicious Transaction Reporting activities are being outsourced by their firm, while only 23% of respondents confirmed that risk assessment activities are being outsourced.

Before placing reliance on an outsourcing service provider, in line with the requirements as set out in firm's CDD procedures and outsourcing framework, policy and procedures, it is best practice for firms to ensure at minimum, that:



The outsourcing service provider is assessed and approved in line with regulated firms outsourcing policies and framework



There is a signed agreement in place with the outsourcing service provider confirming their obligation to comply with the regulated firm's AML/CFT requirements



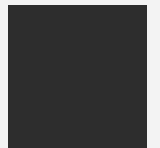
Regular assurance testing can be conducted on the outsourcing service provider to ensure documentation can be retrieved without undue delay

Industry best practice, when undertaking activities on behalf of regulated firms, is for the outsourcing service provider to follow the regulated firm's policies and procedures. Regulated firms must provide regular training to the outsourcing service provider to ensure the appropriate standards are being met.



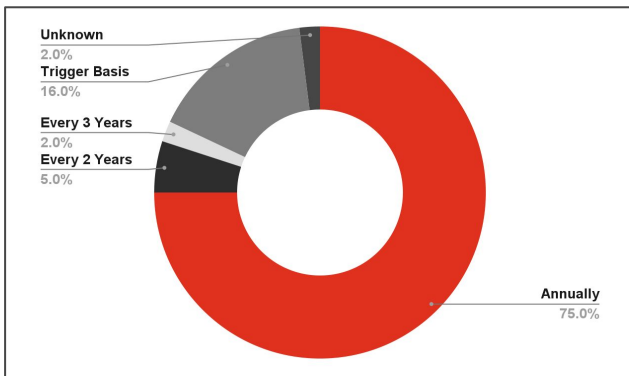
Part 2 Results

Customer Due
Diligence (CDD)

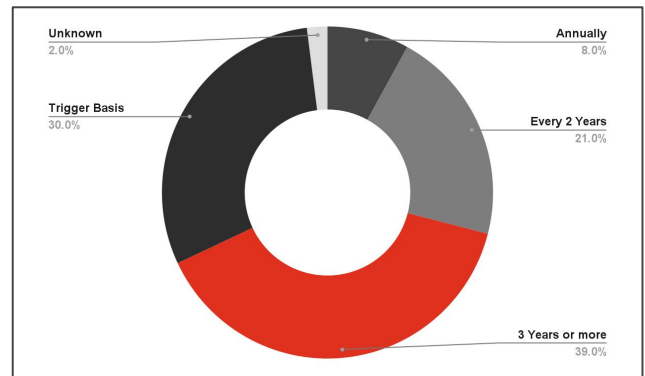


AML Survey results

Part 2 results: Customer Due Diligence (CDD)

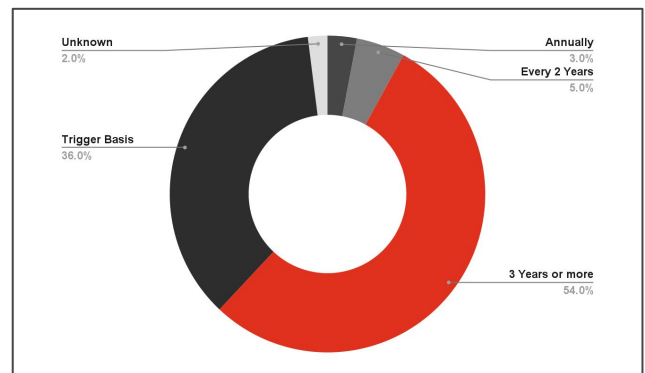


Periodic reviews - high risk customers



Periodic reviews - medium risk customers

The CDD process is considered one of the most integral parts of a regulated entities AML/CFT Framework. This is the process by which entities gather information to know who their customers are and also to understand and document what their expected pattern of behaviour will be, enabling them to identify and report on suspicious activity throughout the customer lifecycle.



Periodic reviews - low risk customers

Know Your Customer (KYC)

The CJA requires regulated entities to keep documents and information relating to their customers up to date. One method by which entities do this is through periodic reviews. Generally firms will take a risk based approach to these reviews, with the most riskiest clients being reviewed on a more regular basis.

AML Survey results

Part 2 results: Customer Due Diligence (CDD)

Know Your Customer (KYC)

High risk customers

The PwC survey found that 75% of all respondents carry out periodic reviews of their high risk customers on an annual basis. While this did not differ significantly across industry types, the survey highlighted that in the E-Money/Payments sector, **this is slightly lower, at 67%**, contrasting with respondents from Credit Institutions, where **100% of respondents** confirmed that they carry out periodic reviews of their high risk customers on an annual basis.

The Central Bank of Ireland (CBI) AML/CFT Guidelines note that the periodic review of customers should be commensurate with the level of ML/TF risk posed by the customer. While the majority of respondents do review their high risk customers on a periodic basis, within the E-Money/Payments sector, 27% of respondents confirmed that reviews of their high risk customers are **only carried out on a trigger basis**.

Medium & low risk customers:

Aligned with the level of risk, the number of respondents who carry out reviews of their medium and low risk customers on an annual basis is much lower than that of high risk customers. **Only 8% of the survey respondents** carry out annual periodic reviews of their medium risk customers, while this is **even lower for low risk clients** at 3%.

Survey respondents noted that trigger reviews are a more common method of keeping customer documents and information up to date for these lower risk customers, with 30% of respondents noting that medium risk customers are kept up to date via trigger reviews, while this is even higher for low risk customers at 36%.

Contrasting with industry types, respondents from Asset & Wealth Management (AWM) entities, were **more likely to confirm the use of “periodic reviews” over “trigger” based reviews** for keeping their customer’s documents and information up to date, with approx. 80% of respondents confirming that their medium and low risk customers were reviewed on a regular basis (every 2 years or more). This is in contrast to the overall response rate, which noted that 69% of medium risk customers were subject to periodic reviews, while overall 62% of respondents confirmed that their low risk customers were subject to periodic reviews.

AML Survey results

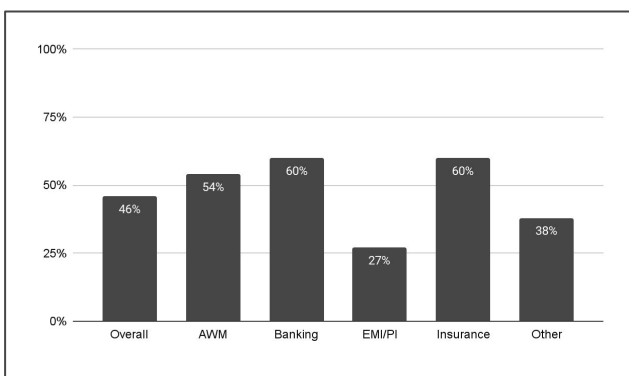
Part 2 results: Customer Due Diligence (CDD)

Know Your Customer (KYC)

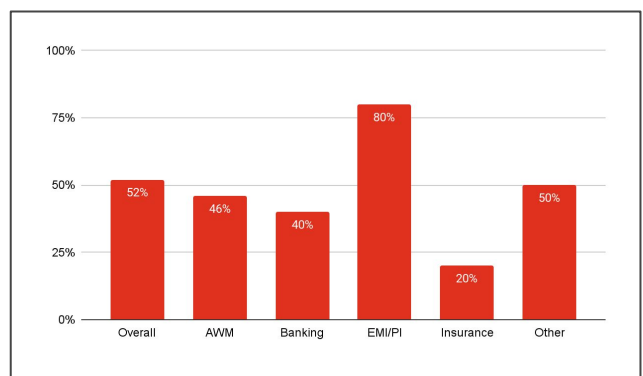
Collection of documents & information

The requirement to collect KYC information both at onboarding and on a periodic review basis is a huge burden for regulated entities. Over the past number of years, a large number of fintech firms have entered the Irish market to **provide automated solutions to regulated entities** when collecting KYC documents, with a focus in particular on providing solutions for the upload of personal identification documents of individual customers. These solutions enable firms to **obtain and analyse documents in real-time** and implement controls, such as liveness checks and biometric verification.

However, it is clear from our survey results that the ongoing review and collection of KYC documents and information remains a huge challenge for regulated entities in Ireland, with a continuous need to review and refresh information held on file for customers. While the collection of KYC documents is becoming more automated across the financial services industry, it is clear from our survey results that non automated methods for collecting this information remains popular, particularly in the more traditional industries, such as Banking and AWM.



Hard copy documents requested



Automated solution to collect KYC

Overall, 52% of respondents confirmed that they have **automated some or all of their KYC collection process**. However, there are significant differences, when this is broken down by industry type where 80% of respondents in the E-Money & Payments sector have automated some or all of their KYC collection process, while this drops to only 20% of respondents from the Insurance sector.

AML Survey results

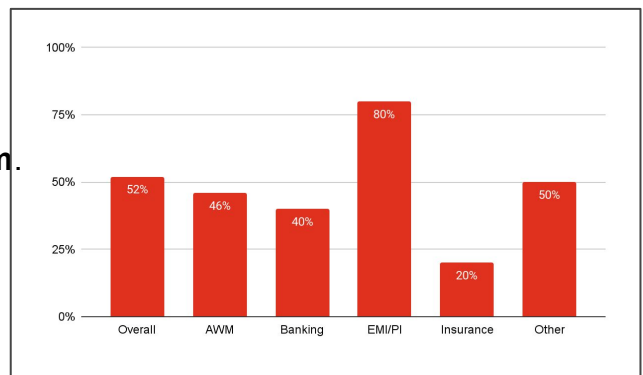
Part 2 results: Customer Due Diligence (CDD)

Know Your Customer (KYC)

Collection of documents & information

Obtaining documents via email also remains a popular method of KYC collection within regulated firms in Ireland, with **72% of respondents overall confirming that this method was used by their firm.**

This approach to the collection of KYC documentation is more popular with more traditional regulated entities. 100% of respondents from the insurance industry confirmed that email is used to collect some or all of their KYC, and 86% of respondents from AWM firms noted this as a method of collection. This is contrasted with **just 40% of EMI/PI firms using email** as a way to collect KYC information.



Collection of documents via email

Similarly the collection of hard copy documents is more popular in these more traditional regulated firms, with 60% of respondents from the Banking and Insurance sectors still collecting hard copy documents for some of their customers, while only 27% of respondents from the E-Money/Payments sector require hard copy documents to be provided by some / all of their customers.

Acknowledging the burden placed on firms by the KYC process, 56% of respondents confirmed that part or all of their KYC / CDD activities have been outsourced (either internally within their group or externally to third parties). This is much higher with E-Money / Payments firms, where 80% of respondents confirmed that part or all of their KYC / CDD activities have been outsourced. It is important to remember that where AML/CFT activities such as this are outsourced, that the regulated entity always remains responsible for ensuring compliance with the obligations contained within the CJA 2010.

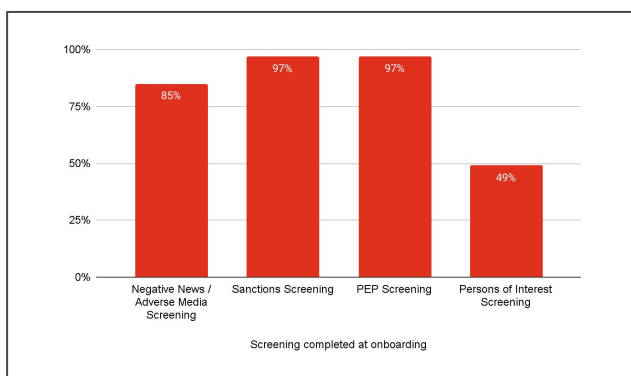
Unsurprisingly, when asked about the scope for further automation in their KYC process, **87% of respondents confirmed that there is scope for further automation within their own KYC processes.** This level of response was similar across all FIs who responded to our survey.

AML Survey results

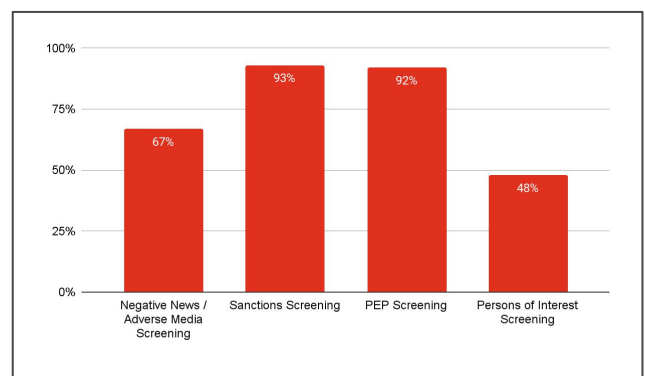
Part 2 results: Customer Due Diligence (CDD)

Screening

Another integral part of the CDD process is the screening of customers, both at onboarding and on an ongoing basis. The screening process is used to identify high risk customer types, such as Politically Exposed Persons (PEPs), enabling an appropriate review of the risk of doing business with a customer to be completed either prior to onboarding the customer or on an ongoing basis when continuing a relationship with a customer.



Onboarding screening completed



Ongoing screening completed

Through the survey, **97% of respondents confirmed that PEP and Sanctions screening is completed at the onboarding stage** of their CDD process. There is a slight drop in these rates for ongoing screening, with 93% of respondents confirming that Sanctions screening is completed on an ongoing basis, and 92% of respondents confirming that PEP screening is completed on an ongoing basis.

While Negative News screening is also completed by the majority of respondents (85%) at the onboarding stage, there is a **drop to 67% of respondents who complete Negative News screening on an ongoing basis**. Approximately 50% of respondents confirmed that “persons of interest” screening is also part of their screening process, both at onboarding stage and on an ongoing basis.

The majority of regulated entities who responded to this Survey (74% of respondents) **complete their ongoing screening on a nightly basis**, while most other respondents confirmed that their ongoing screening is completed either on a weekly (7% of respondents) or monthly (13% of respondents) basis. 100% of respondents from the Banking industry confirmed that ongoing screening is completed on a nightly basis.

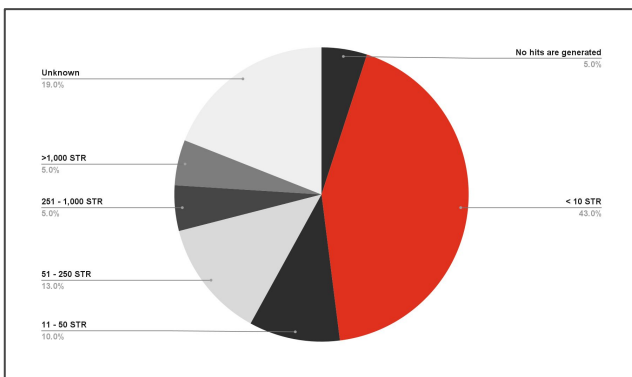
AML Survey results

Part 2 results: Customer Due Diligence (CDD)

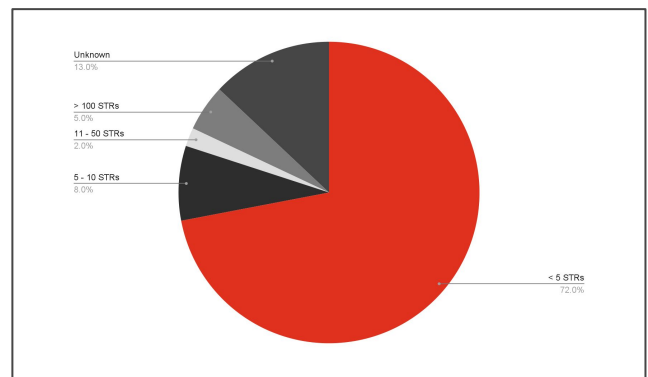
Screening

The reviewing and dismissing of potential hits can be a very labour intensive task within the CDD process, therefore the fuzzy logic tuning of screening systems is very important to ensure that all potential hits are being alerted while also ensuring that screening teams are not reviewing an unnecessarily high number of alerts that may become unworkable during the normal course of business. While a high proportion of respondents were not aware of the fuzzy logic used within their systems, where this was known 62% of respondents confirmed that their fuzzy logic for customer screening was > 90%, while 52% of respondents also confirmed > 90% for their sanctions screening fuzzy logic. Only 14% of respondents noted that their fuzzy logic was <80% for both sanctions and customer screening.

Suspicious Transaction Reporting



Suspicious Transactions flagged internally monthly



Suspicious Transactions reported to external authorities monthly

Regulated entities are required to report to external authorities transactions that are complex, unusual or where they do not have an apparent economic or lawful purpose. In order to ensure effective reporting of these transactions, it is important that FIs have well documented processes and reporting lines in place to ensure that suspicious transactions or behaviour can be reported and reviewed in a timely manner.



AML Survey results

Part 2 results: Customer Due Diligence (CDD)



Suspicious Transaction Reporting

43% of respondents to the survey confirmed that **<10 suspicious transactions are flagged through their firms' internal suspicious transaction reporting processes** on a monthly basis. However, variances are noted across the various entity types, with 100% of respondents from the insurance sector noting that <10 suspicious transactions are reported on a monthly basis, while 60% of respondents from the Banking industry confirmed that >1,000 suspicious transactions are reported monthly.

Aligned to the number of internal suspicious transactions being reported, 60% of respondents from the Banking industry reported that >100 Suspicious Transaction Reports (STRs) are made externally to the authorities on a monthly basis. Similarly 100% of respondents from the Insurance sector reported that <5 STRs are reported externally on a monthly basis. 72% of respondents overall confirmed that **<5 STRs are reported to external authorities monthly**.



Part 3 Results

AML / CFT Business
Wide Risk Assessment
(BWRA)



AML Survey results

Part 3 results: AML / CFT Business Wide Risk Assessment (BWRA)

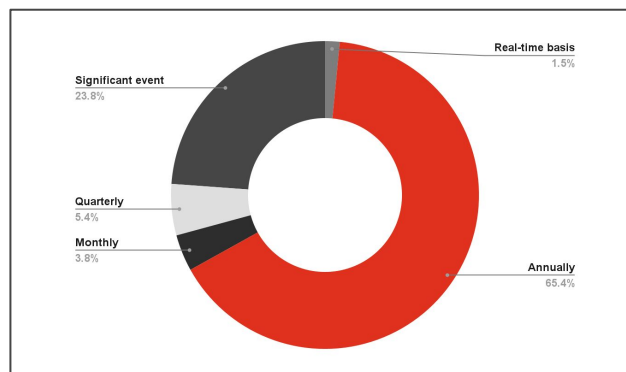
AML/CFT legislation and guidance, both locally in Ireland and at a European Level is centred around regulated firms adopting a risk based approach to Money Laundering and Terrorist Financing (ML/TF). This means that firms are required to know and understand the ML/TF risks associated with their particular business and apply appropriate controls to manage these risks. There is no one-size fits all approach to managing ML/TF risks.

Section 30A of the CJA 2010 requires firms to carry out an assessment (in the Act referred to as a 'business risk assessment') to identify and assess the risks of money laundering and terrorist financing involved in carrying on their business activities, taking into account a variety of risk factors, such as customers, product, geography, etc.

The AML / CFT Business Wide Risk Assessment (BWRA) enables firms to:

-  Identify areas of highest ML/TF risk within their business and ensure appropriate resources are allocated on a risk based approach to these areas;
-  Identify gaps and areas for improvement in AML / CFT policies, procedures, processes and controls;
-  Ensure that senior management are equipped to make informed decisions about risk appetite and the implementation of controls, allocation of resources and spend on technology to mitigate risk.

Firms should ensure that their BWRA is tailored to their business, carried out on at least an annual basis and that it takes account of risks in line with various Irish and International Legislation and Guidance.



Frequency of AML/CFT BWRA

AML Survey results

Part 3 results: AML / CFT Business Wide Risk Assessment (BWRA)

AML/CFT BWRA owners

An effective AML/CFT BWRA framework is one where there is ownership and involvement across both the first and second line of defence, ensuring that risks are identified and managed in an effective manner.

First line of defence



In practice the role of the first line of defence in the BWRA should be in the identification and ownership of ML/TF risks. The first line of defence should be best placed to identify risks with products, customers, etc., and also to own and monitor controls which have been implemented to manage these risks.

Second line of defence

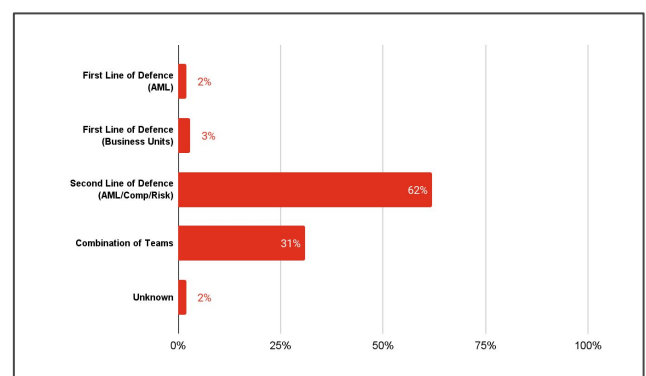


Generally, the role of the second line of defence in the BWRA is in the development, implementation and oversight of the BWRA framework

The involvement of both the first and second line of defence in the BWRA encourages a **more holistic approach** to the risk assessment process and enables Senior Management and the Board to make informed decisions on where to prioritise resources to manage and mitigate ML/TF risk.

62% of all respondents to the survey confirmed that their second line of defence is responsible for completing their AML/CFT BWRA, while 31% of respondents noted that their firm uses a combination of first and second line to carry out this process.

100% of respondents from Credit Institutions, noted that they used a combination of teams from first and second line to complete their BWRA. Our experience across the industry is that a combination of teams working together will produce the **most accurate overview and assessment of ML/TF risk** within their business.



AML/CFT BWRA - owners

AML Survey results

Part 3 results: AML / CFT Business Wide Risk Assessment (BWRA)

AML/CFT BWRA owners

When developing and managing the AML/CFT BWRA methodology, the following measures should be considered by those involved in the process:

The risk criteria which should be assessed during the BWRA process, being mindful of applicable Irish and international legislation / guidance / papers;

Whether risk factors should be weighted differently depending on their relative importance;

Whether any AML/CFT events that occurred in the previous year will have a significant impact on the BWRA process;

How risks should be assessed, including how you will assess if any risks have increased or decreased since the previous BWRA was executed;

How controls should be assigned and evaluated for all risks;

How remedial actions and risk managers are assigned as needed.

Method used to complete the BWRA

The BWRA process can be highly manual and time consuming for firms to complete due to the requirement to gather large volumes of data from potentially multiple sources within their business. The use of digital tools can greatly improve the efficiency of this process, however, it is clear from our survey results that regulated firms in Ireland are still heavily reliant on manual methods to complete their BWRA.

AML Survey results

Part 3 results: AML / CFT Business Wide Risk Assessment (BWRA)

Method used to complete the BWRA

Our survey found that **75% of firms across all sectors have a fully manual BWRA process**, with 100% of survey respondents from the insurance sector noting that their BWRA process is manual. This is **much lower for more recent entrants to the market**, where only 53% of EMI/PI firms confirmed that their BWRA process is fully manual. 33% of these firms noted that their BWRA process is partially automated, while 13% rely on a fully automated process. This is contrasted with the overall results, where only 3% of firms rely on a fully automated BWRA process, with 20% of all respondents noting that their BWRA process is partially automated.

The use of digital tools and automation can not only lead to a much more efficient process, it can also result in a more accurate representation of the risks within a business, with less reliance on human input and interpretation. The benefits of an automated BWRA process include:



Reduced risk associated with the manual interpretation and input of data sets;



Reduction in resource allocation due to efficiencies gained from automation;



More accurate and reliable information collated from multiple sources in one location;



Improved compliance requirements with regard to record keeping and data traceability.

BWRA frequency and approval

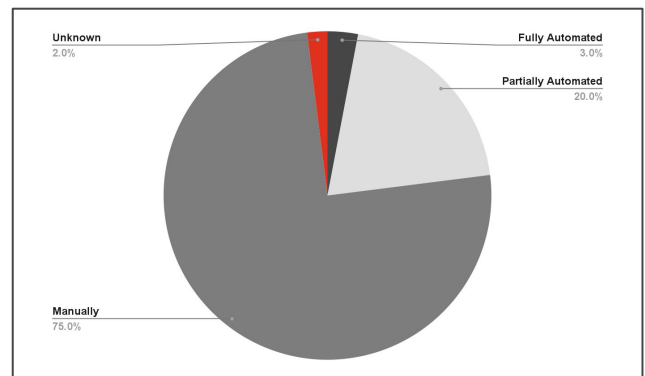
Unsurprisingly, when asked about the frequency of the BWRA, the majority of the survey respondents (85%) disclosed that they **execute their BWRA on an annual basis**. This is relatively consistent across all entity types with 100% of respondents from Credit Institutions noting that they complete their BWRA on an annual basis. It was also noted by 31% of respondents that they **re-execute their BWRA following a significant change** within their business. This was slightly higher within EMI/PI firms, where 47% of respondents noted that they re-execute their BWRA following significant changes within their business. A small number of respondents confirmed that their BWRA is carried out on a more frequent basis (monthly - 5% / quarterly - 7%).

AML Survey results

Part 3 results: AML / CFT Business Wide Risk Assessment (BWRA)

Method used to complete the BWRA

Only 2% of respondents have **implemented a real-time BWRA process** within their firm. The benefit of a real-time BWRA process is the **automatic rescoring of risks** when significant changes / events occur within a business. This use of real-time risk scoring means that significant manual / human intervention is not required and it allows firms to quickly identify new / emerging AML/CFT risks and trends within their business.



Methods used to complete the BWRA

93% of respondents to our survey confirmed that their AML/CFT BWRA is **approved by their Board**. This is an expected outcome in line with the CJA requirement for firms to present the BWRA results to the Board on an at least annual basis for discussion, challenge and final approval. Risk assessments are only effective and relevant if they're kept up to date.

BWRA impact on AML/CFT activities

To ensure that your firm is appropriately managing your risk, it is important that action is taken from the outcome of your BWRA. The CBI Guidelines note that “a Firm’s Business Risk Assessment should identify the ML/TF risks, which the Firm is potentially exposed to and, in accordance with the Firm’s risk based approach, outline where resources need to be prioritised in order to counter ML/TF”. Some of the areas highlighted in the guidance includes:

“Firms should rely on their assessment of the risks inherent in their business to inform their risk-based approach to the identification and verification of an individual customer.

Transaction Monitoring controls should be “fully reflective of the risks identified in the Firm’s Business Risk Assessments and Customer/Transaction Risk Assessments

While 20% of respondents were not aware if their BWRA impacted on other aspects of their AML/CFT programme, the majority of respondents did note that their BWRA influenced other areas, with the Customer Risk Assessment being the area most impacted by the BWRA.



Part 4 Results

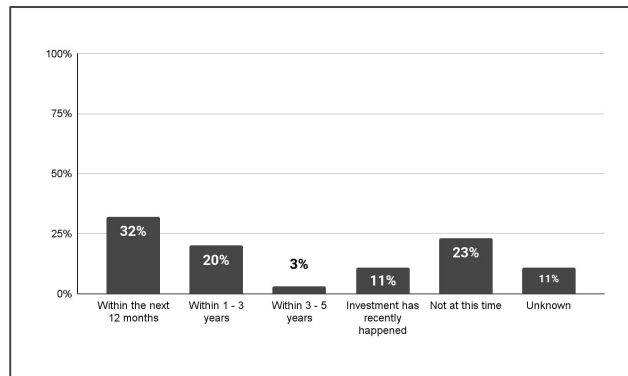


Technology Analysis



AML Survey results

Part 4 results: Technology analysis



If and when firms consider investing in new AML/CFT Technology

Key takeaways



Our Survey found that 15% of Survey respondents disclosed that they have no automated systems in place to manage their AML/CFT process.



30% of respondents have multiple AML/CFT systems that are not interconnected.



51% of survey respondents disclosed that they are planning to invest in their AML/CFT technology within the next 3 years.

AML Survey results

Part 4 results: Technology analysis

AML / CFT technology infrastructure

The use of technology within regulated firms in Ireland to manage AML/CFT processes has increased exponentially over the last few years with a large focus by firms on considerably reducing operational costs, leveraging the use of data analytics to better identify risk and achieve a single customer view to better understand customers and the AML/CFT risk they pose. Without appropriate technology, firms are relying on **very manual, labour intensive processes**, which can be highly repetitive. This can lead to duplication of effort, as well as an increased risk of errors due to the manual nature of the process.

The use of automation and technology within AML/CFT systems and processes can provide immediate value to firms, including:



Live customer due diligence application;



Powerful, interactive, user friendly reporting;



Faster data gathering;



Consistent, complete and accurate calculations - removing human error;



Full audit trail for future assurance and review.

With this increased use of technology, it is not surprising that 84% of respondents to our survey confirmed that they have some form of automation/technology in place to manage their AML/CFT processes. However, when you delve into this figure further, it is clear that there is still room for improvement in the AML/CFT tech infrastructure in place in regulated entities in Ireland.

31% of survey respondents described their AML/CFT tech infrastructure as being **based on multiple interconnecting AML/CFT systems**, while 30% of respondents described their tech infrastructure as being **multiple AML/CFT systems, which are not interconnected**. This was particularly the case with respondents from credit institutions, where 80% of respondents described their AML/CFT tech infrastructure this way.



AML Survey results

Part 4 results: Technology analysis



AML / CFT technology infrastructure

Over recent years there has been a huge increase in the number of vendors on the market providing AML/CFT technology solutions, which can lead to **challenges in selecting the right systems and vendors for your particular business**. When designing your technology strategy, it is not necessary to have one system that addresses all of your AML/CFT requirements, however, it is important to have a **coordinated strategy** in place, which is built around one or a number of core processes / systems such as account opening, screening and risk rating. Where a coordinated AML/CFT technology strategy is not in place, it can lead to challenges managing AML/CFT risks as it can be more difficult to collate information and obtain a single customer view / golden source of truth.

While the majority of respondents to our survey do have some level of automated systems in place to manage their AML/CFT processes, a higher proportion of firms (63%) in the Credit Union & Credit Servicing sectors describe themselves as having no automated systems in place.

Further emphasising the room for enhancements in relation to AML/CFT technology, 51% of the respondents to our survey confirmed that they are considering **investing in new AML/CFT technology over the next 3 years**, with 31% of respondents identifying that this is something that they are **considering doing in the next 12 months**. This is particularly the case for credit institutions with 60% of respondents noting that this is a consideration for them this year.

Of the respondents who noted that they are considering investment over the 12 months, 84% already have some form of AML/CFT technology in place, either in the form of one core system (16% of respondents) or multiple AML/CFT systems which are interconnected (37% of respondents) or not interconnected (32% of respondents).

11% of respondents to our survey confirmed that they have recently made investments in their AML/CFT technology, while **23% confirmed that they are not considering any investment at this time** - this was slightly higher in the insurance sector, where 40% of respondents confirmed this.

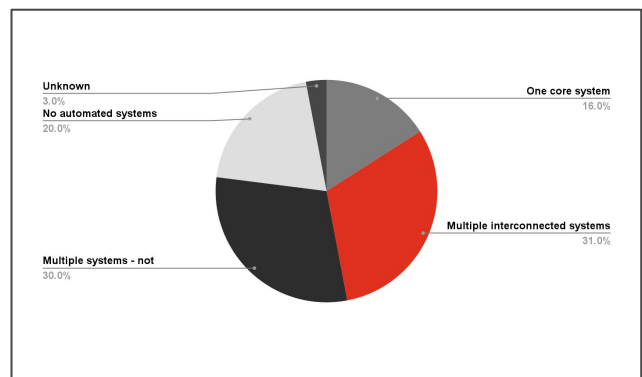
Our survey found that **87% of firms believe that there is scope for further automation to improve their onboarding process**, with all respondents in Credit institutions confirming this. This is a significant number considering the relevance of the customer onboarding process.

AML Survey results

Part 4 results: Technology analysis

AML / CFT technology infrastructure

Emphasising the importance of investing in and embracing AML/CFT technology, the Financial Action Task Force (FATF) released a paper on the opportunities of new technologies for AML/CFT in 2021 which highlighted that technology can make AML/CFT measures faster, cheaper and more effective. They also noted that innovative skills, methods, and processes, as well as innovative ways to use established technology-based processes, can help regulators, supervisors and regulated entities overcome many challenges.



AML / CFT Tech infrastructure/systems

AML/CFT activities supported by technology/systems

Unsurprisingly, Customer Screening was the most popular activity selected by respondents to our survey (77% of respondents) as an activity that is supported within their firm by AML/CFT technology / systems. Transaction Monitoring was also popular amongst respondents (61% of respondents), however, variances were noted across the industry types, with 100% of respondents from Credit Institutions and EMI/PI firms confirming that this technology / system is in place, with only 54% of respondents from AWM firms and 20% of respondents insurance firms confirming this. Risk Assessment activities, both from a business and customer perspective are an area of focus for regulators and regulated entities, however, it is clear from our survey results that **this is an area that remains highly manual for firms**. This is particularly true for the Business Wide Risk Assessment, where only 7% of respondents confirmed that they have a system in place to manage this process, albeit this is slightly higher for EMI/PI firms, where 20% of respondents confirmed that they have technology in place to manage this. While there was a slightly higher number of respondents confirming that they have systems / technology in place for their customer risk assessment (38% of respondents), this was also variable across the industry types, with a higher number of respondents from Credit Institutions (60%) and EMI/PI firms (80%) confirming this technology as being in place, with only 20% of respondents from AWM and Insurance firms noting the use of technology for the customer risk assessment process.

AML Survey results

Part 4 results: Technology analysis

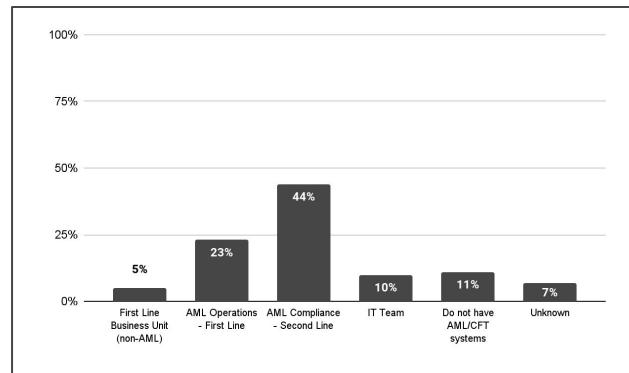
Ownership of AML/CFT infrastructure

Traditionally IT infrastructure and systems would have been seen as sitting exclusively with IT Departments within regulated institutions, however, we are now seeing this become more integrated with the business, which can lead to a **greater understanding of the risks and benefits associated with AML/CFT technology**.

Our survey found that in 44% of firms, AML/CFT technology is owned by the AML Compliance team in the second line of defence. This can include the ownership of activities such as the management of rules, upgrades, etc. This is slightly higher in the EMI/PI sector (60% of respondents) and the Insurance sector (80% of respondents). Interestingly AML/CFT technology is owned by IT Teams in only 10% of respondents to our survey, with 85% of these respondents coming from the AWM sector.

Ultimately, where ownership of your AML Technology sits is a matter for individual firms to decide, however, what is important is that as a firm, you **fully understand the impact of the technology on your firm's regulatory compliance** and that there is also an appropriate level of governance and oversight on your AML/CFT technology infrastructure.

To ensure the effectiveness of an organisation's AML/CFT infrastructure, the board and senior management need to be able to rely on adequate line functions – including monitoring and assurance functions – within the organisation. AML/CFT infrastructure ownership is key within firms to understand **who owns and manages the risks but also who oversees this**.



Ownership of AML/CFT Infrastructure



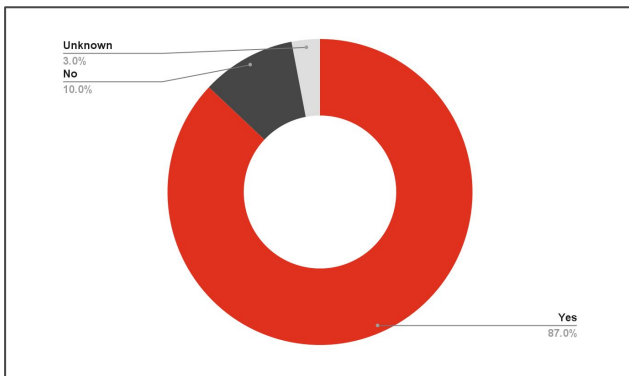
Part 5 Results

Management
Information

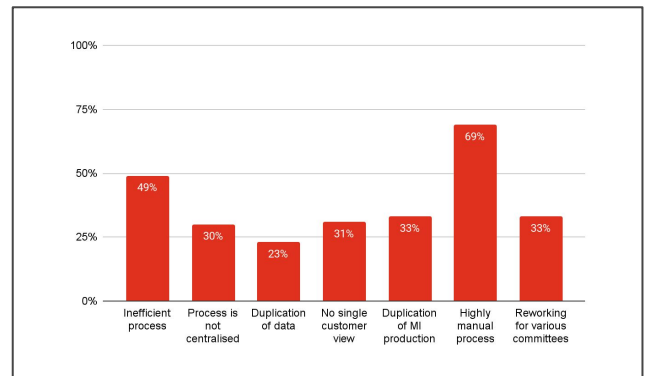


AML Survey results

Part 5 results: Management Information



MI & reporting challenges



Key challenges for data & MI reporting capabilities

Comprehensive and relevant Management Information (MI) is crucial for regulated entities to ensure that AML/CFT controls are operating as expected, as well as to assist with identifying potential issues or areas of concern before they occur. Within organisations, MI can often develop and grow organically over a long period of time, with additional data points being added without considering the implications of managing this on an ongoing basis. We also know that regulated entities can spend a significant amount of time tweaking MI for numerous committees and meetings, leading to **additional work but oftentimes not a huge amount of value added**. All of this aligns with the responses to our survey, where **87% of respondents reported challenges** with their MI & Reporting processes.

The most common MI & Reporting challenges highlighted by FIs in our survey were:



Highly Manual Process - 69% of respondents noted that this was a challenge for their firm;



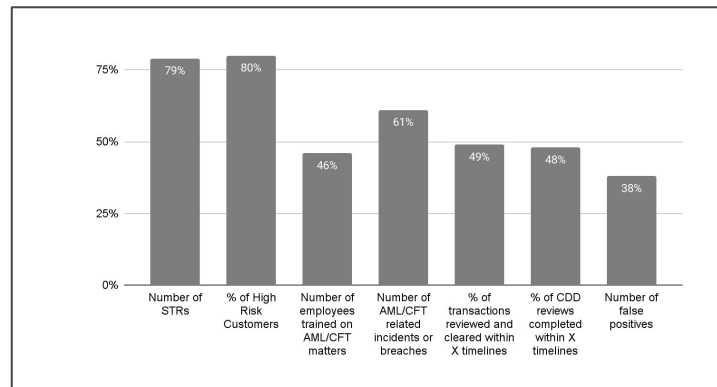
Inefficient Process - linked to the highly manual nature of the production of AML/CFT MI within FIs in Ireland, 49% of respondents confirmed that their MI & Reporting process was inefficient;



Duplication / Reworking MI - 33% of respondents noted that they are required to rework MI for various and that duplication of MI is an issue within their firm.

AML Survey results

Part 5 results: Management Information



AML/CFT KPI Insights

AML/CFT MI must be sufficiently detailed to ensure that senior management is able to make timely, informed and appropriate decisions on AML/CFT matters. According to our survey responses, the most common AML/CFT KPIs reported on by FIs are the **% of High Risk Customers onboarded** (80% of respondents) and the **number of STRs** (79% of respondents) each month. 61% of respondents also noted that their MI provides data on the number of **AML/CFT related incidents or breaches**. Less than half of firms who responded to our survey include AML/CFT KPIs on areas such as employee AML/CFT training, % of transactions/CDD reviews completed within SLA and the number of false positive hits alerted by transaction monitoring systems.



AML Survey results

Conclusion

New Individual accountability for senior management may result in personal monetary penalties

The new Senior Executive Accountability Regime (SEAR) holds the Head of Anti-Money Laundering responsible for managing the AML/CFT function. The regulator can now take enforcement action against that individual leading to personal monetary penalties.

AML regulations are ever increasing in an attempt to keep pace with financial crimes. Ireland has pitched to host the new EU AML Authority (AMLA) which will be established in 2024. This will become a European Regulator supervising anti-money laundering compliance across all member states and will issue a new common rule book. This will only increase the requirements to combat financial crime.

With both SEAR and a new EU Regulator on the way, having a robust AML framework is crucial in managing the threat of financial crime. Increasing automation can support better governance, reporting and overall management of risk enabling senior management to discharge their individual accountability.

Sinead Owenden noted: “Ireland continues to progress in strengthening measures to tackle money laundering and terrorist financing and has received an increased rating in the most recent inspection by the global Financial Actions Task Force in 2022.

“Technology is the only way to keep up with the race against financial crime and there is much more to do on automation. Many clients have invested over the years but the key to success is a fully integrated technology system. Disparate technology makes it more difficult to gather information, identify suspicious activity and report financial crime.”

About the survey

This survey was carried out amongst regulated Irish financial services firms in Summer 2023 having participants across the funds, banking, E-money, payment, insurance and credit servicing industry. The aim of the survey was to identify the extent of the challenges and opportunities for regulated financial services institutions in the management, identification and oversight of anti-money laundering and financing terrorism in the light of a new regulation and increased supervision coming in 2024.

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 152 countries with nearly 328,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

03

Key actions businesses can take today



Key actions businesses can take today

Be prepared

1

With a new EU regulator on the way, having a robust AML/CFT framework is crucial in managing the threat of financial crime. To ensure your AML/CFT framework is set up for success, review the following areas for gaps and enhancement opportunities:



Governance and oversight;



People and capabilities, ensuring clearly defined roles and responsibilities across the three lines of defence;



Risk-based approach; and



Processes and controls.

Emerge stronger

2

Without reliable data and innovative technology, regulated entities in Ireland cannot effectively respond and adapt to emerging AML threats. Over the next three years, more than half of firms will invest in their AML/CFT technology.

Before you do, assess your firm's current infrastructure. Sometimes, enhancements to existing technology can be as efficient and effective as new technology—and a significant cost-saving.



We are here to help you



Our specialised team has vast experience and expertise in AML and can help firms address new and existing money laundering and terrorist financing risks. We can help you create an AML-focused risk management plan; conduct large-scale AML remediation programmes; assess and enhance your firm's AML framework; develop and review your AML compliance monitoring programmes; and transform your AML and financial crime target operating model. Contact us today to discuss any of these challenges and explore our solutions in more detail.



Sinéad Ovenden

Financial Service Regulatory Partner

sinead.m.ovenden@pwc.com



AML

Thank You

www.pwc.ie

© 2023 PwC. All rights reserved. Not for further distribution without the permission of PwC. “PwC” refers to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL), or, as the context requires, individual member firms of the PwC network. Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm’s professional judgment or bind another member firm or PwCIL in any way.