fscom
Expertise that adds value.

Fincrime Compliance Report 2022

An insight into AML audits and the compliance challenges facing financial services firms

July 2021 – July 2022

Contents

Foreword

We are delighted to present fscom's Fincrime Compliance Report for 2022. It's been five years now since we issued our last audit analysis report. Even setting aside major global events like the COVID-19 pandemic, it would be an understatement to say a lot has changed since then. The continued rise of technology is one example. Money launderers are using increasingly sophisticated tools to conceal illicit financial flows, while regulators increasingly expect firms to use technology to detect suspicious activity.

fscom is uniquely placed to evaluate and interpret relationships between regulation and practical implementation, and the subsequent analysis of results. With a wealth of compliance experience and a deep understanding of our client's business objectives, we work closely with our clients to grasp how regulations apply to them. We regularly carry out audits of clients from all types of financial services institutions to assist them to consistently improve their framework to combat financial crime. This gives us an unrivalled insight into the issues firms are facing around regulatory compliance.

Client confidentiality is paramount and we would never disclose any findings of a particular audit. However, in the course of auditing, we often notice similar themes and challenges facing firms that sometimes impedes compliance. This report distils and analyses that insight to pull out key trends in firms' financial crime compliance.

In the coming pages, we summarise the most common weaknesses in internal compliance systems identified in 57 audits that we carried out between July 2021 and July 2022. This data analysis is combined with our sector expertise to produce a report which we are confident will assist clients and industry stakeholders and enable firms to benchmark themselves using industry standards.

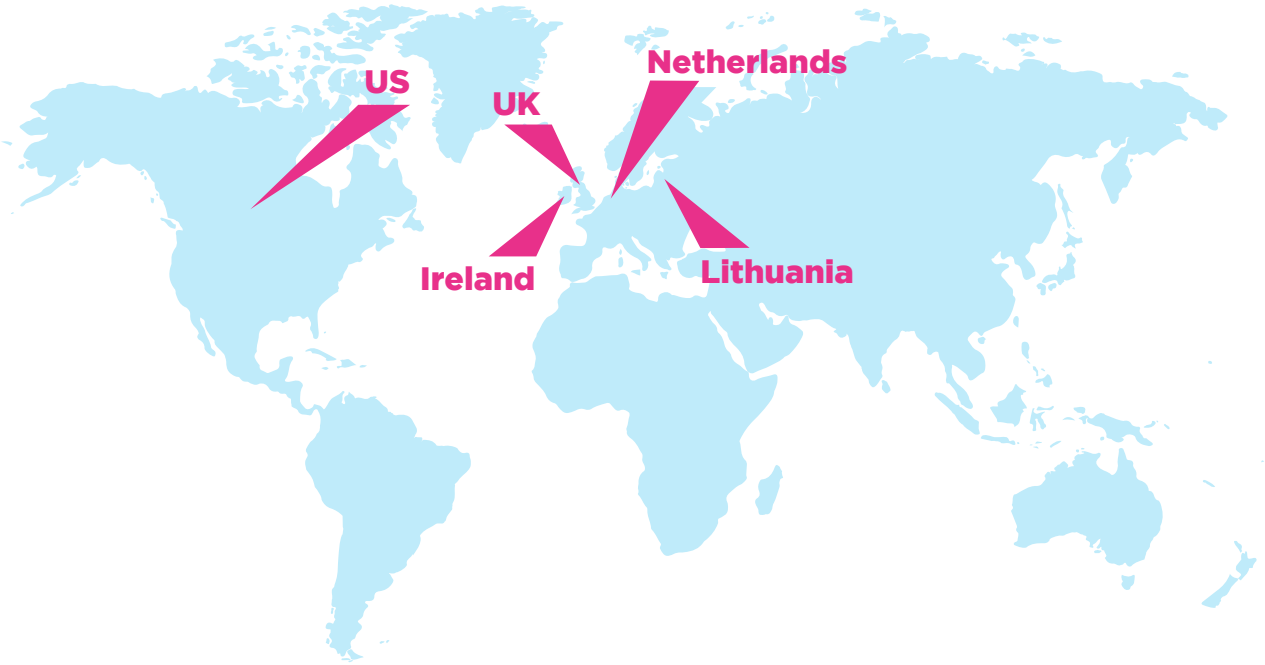
This report does not constitute the giving of advice, and fscom accepts no liability, without limitation, for actions or outcomes based on findings or opinions within the report. Nonetheless, its findings may prove valuable for firms who are in the process of rethinking their AML compliance processes.

If you have any questions about this report or how fscom can help you or your firm, please contact us and we will be more than happy to help you with your compliance needs and enquiries.

Overview

This report analyses anti-money laundering (AML) compliance audits which fscom carried out and finalised from July 2021 to July 2022. The 57 reviews were conducted across a range of financial services institutions including:

- electronic money institutions (EMIs)
- authorised payment institutions (APIs)
- cryptoasset firms (registered, temporarily registered, and unregulated) and;
- unregulated firms with internally adopted standards to adhere to local legislation and guidance.



While the majority of the 57 firms reviewed were UK-based and therefore adhering to UK specific regulations and guidance, several reviews were carried out for firms in the jurisdictions of the US, Ireland, Netherlands and Lithuania.

Reviews for non-UK-based firms were carried out in reference to the local applicable legislation and guidance.

The purpose of this report is to provide data and information regarding the specific areas of these 57 firms' AML frameworks which have been identified as requiring further review and enhancement. The report will also provide guidance and recommendations regarding how companies should address these issues to improve their regulatory compliance.

Regulatory citations and guidance cited in this report have been made in reference to:

- Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (amended) (MLRs),
- The Joint Money Laundering Steering Group (JMLSG) Guidance for the UK Financial Sector, 2020 Revised Version,
- Financial Crime Guide: A firm's guide to countering financial crime risks (FCG) (published by the FCA),
- Wolfsberg Group Guidance on Digital Customer Lifecycle Risk Management, and
- Proceeds of Crime Act 2002.

Overview of fscom's AML Audit Process

This section breaks down fscom's approach to carrying out an AML audit, and how we assess a firm's compliance.

The audit testing process consists of four key elements:

1. **The review of all AML/CTF policy and procedural documentation** – this initial off-site document review allows for an assessment of the firm's internal policies and procedures against all applicable regulatory obligations and approaches as set out within relevant industry guidance.

2. **'Side-by-side' walkthroughs** – this relates to conducting 'over-the-shoulder' walkthroughs of all relevant procedures, systems, and controls, in order to assess their operational efficacy.

3. **Testing** – taking a representative sample of the firm's customer base. Then, the auditor tests the customer due diligence, transaction information and documentation held against the firm's internal policies and procedures and all applicable regulatory obligations and approaches as set out within relevant industry guidance. We will also test your PEP, Sanctions and adverse screening to ensure it is working as expected.

4. **Staff interviews** – this relates to conducting sit-down interviews with the firm's employees to gauge their knowledge of the legislation and their own responsibilities within an AML Framework. This also allows fscom to make a determination on the 'culture of compliance' promoted within the firm and on the efficacy of the firm's top-down approach and senior management buy-in as it relates to AML compliance.

Following the completion of the testing process, a draft report is presented to the client which constitutes 3 elements:

- Executive summary,
- High and low impact findings, and
- Current state and best practice recommendations.

Following the issuance of a draft report, clients are encouraged to provide feedback or challenge to any findings, before a final version is completed with the addition of the firm's management responses to each of the high and low impact findings.

High and Low impact findings

When rating any findings identified, fscom has developed a scoring methodology which considers two key elements:

- Level of compliance, and
- Impact.

The level of compliance is derived across 4 broad ratings:

1	**Compliant** the process covers all regulatory requirements and financial crime controls are appropriate and effective.
2	**Compliant with improvements** the process is primarily compliant, with minor improvements based on best practice recommended to develop further.
3	**Partially non-compliant** tone or more low-impact issues are identified within a process or policy and/or procedures which pose an element of regulatory risk but are not considered to be significant and, as such, do not constitute a systemic breach.
4	**Significantly non-compliant** one or more high-impact issues are identified within the process or procedures causing material non-compliance against regulatory requirement.

The impact score is rated from 1 – 5 (1 being the lowest impact and 5 the highest impact) based on the likelihood of its occurrence and the impact for the firm.

While the level of compliance is generally a static rating across all firms, the impact score is subject to change based on several factors, most notably, the size and nature of the firm being audited.

The statistics analysed within this report are based on the high and low impact findings identified and recorded across the 57 audit reports issued by fscom.

Audit review and testing areas

The high and low impact findings have been attributed to the following 13 areas which fscom's auditors will test and review during the process:

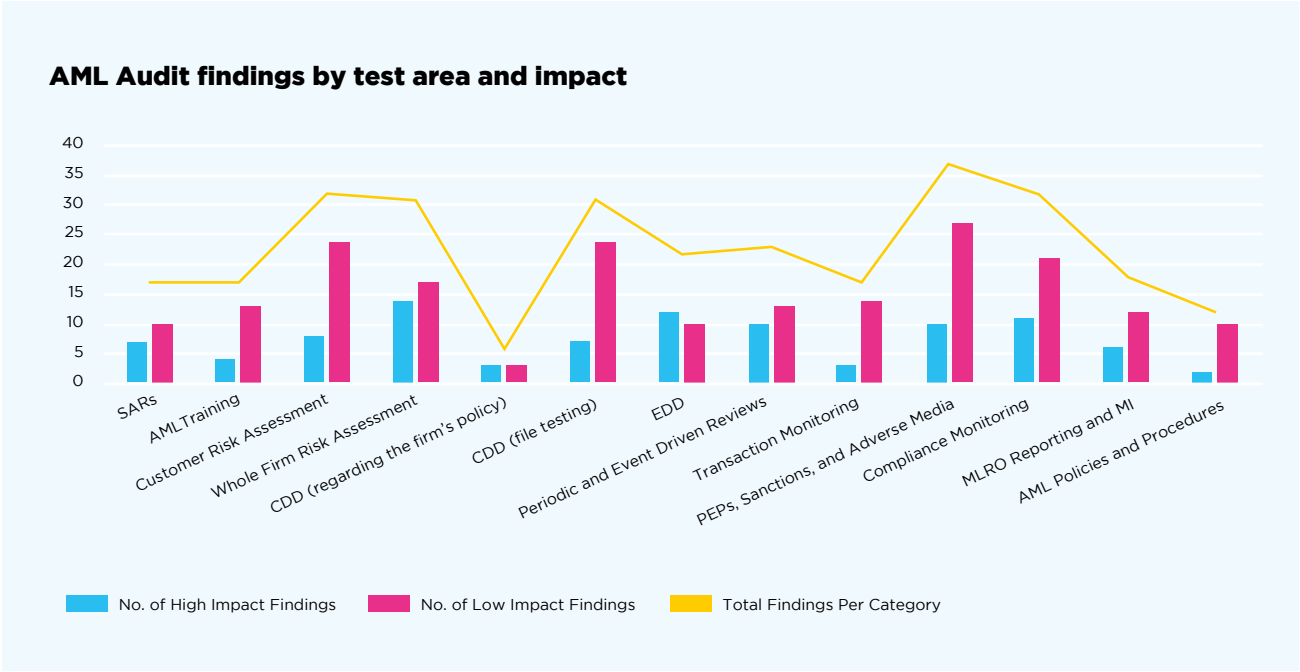
- ✔ Suspicious Activity Reporting (SARs),
- ✔ AML Training,
- ✔ Customer Risk Assessment,
- ✔ Whole Firm Risk Assessment (WFRA),
- ✔ Customer Due Diligence (CDD) – regarding the firm's policy,
- ✔ CDD – file testing,
- ✔ Enhanced Due Diligence (EDD),
- ✔ Periodic and Event Driven Reviews,
- ✔ Transaction Monitoring,
- ✔ PEPs, Sanctions, and Adverse Media,
- ✔ Compliance Monitoring,
- ✔ MLRO Reporting and Management Information (MI), and
- ✔ AML Policies and Procedures.

Statistical overview

Across the 57 audit reports issued, 295 findings were recorded (on average 5.18 per audit), 97 of which were recorded as high impact findings (1.70 per audit) and 198 of which were recorded as low impact findings (3.47 per audit).

The findings were distributed across the 13 review and testing areas as follows:

Audit Review and Testing Areas	No. of High Impact Findings	No. of Low Impact Findings	Total Findings Per Category
SARs	7	10	17
AML Training	4	13	17
Customer Risk Assessment	8	24	32
WFRA	14	17	31
CDD (regarding the firm's policy)	3	3	6
CDD (file testing)	7	24	31
EDD	12	10	22
Periodic and Event Driven Reviews	10	13	23
Transaction Monitoring	3	14	17
PEPs, Sanctions, and Adverse Media	10	27	37
Compliance Monitoring	11	21	32
MLRO Reporting and MI	6	12	18
AML Policies and Procedures	2	10	12
Total	**97**	**198**	**295**



Top 5 most affected review and testing areas

This section identifies the five key areas of compliance where deficiencies and other findings were most often identified during our audits. The following sections look at other areas where findings are less common, but still should not be ignored.

Based on the data shown in the table and graph above, more than 30 findings were recorded across each of the following five review and testing areas:

Customer Risk Assessment (32),

Whole Firm Risk Assessment (31),

CDD (file testing) (31),

PEPs, Sanctions, and Adverse Media (37), and

Compliance Monitoring (32).


0 11 0010
1 1
1 0

1. Customer Risk Assessment

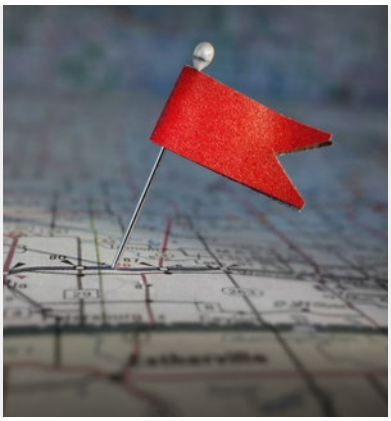
32 findings were identified in relation to firms' customer risk assessments, eight of which were recorded as high impact and 24 of which were recorded as low impact. Of the 32 findings, 27 were found to be deficient based on the following four factors:

Finding Evidence	No. of Audits Affected
Output of the risk assessment is not conducive to a robust risk based approach	3
The risk assessment does not consider some key risk indicators identified by the firm within their WFRA	5
The risk assessment does not consider a wide enough range of risk factors	7
The firm's country risk assessment fails to adequately consider all high risk third countries (HR3Cs) and/or the scoring methodology would not ensure that mandatory EDD measures are applied when entering a business relationship (or a transaction) involving these countries	12

Of the four factors, we note that the issue most identified was regarding firms' country risk assessments. Specifically, the finding relates to HR3Cs as published by HM Treasury and specified in schedule 3ZA of the MLRs (HR3Cs in Europe are published by the European Commission).

The two main issues were:

- Firms had failed to ensure their country risk assessment was kept up to date with changes made by HM Treasury or the European Commission, and/or
- The scoring methodology used within the holistic customer risk assessments failed to ensure EDD would be applied where a customer (or transaction) was to be established in a HR3C.



While the law does not state that HR3Cs must be risk rated as high by firms, there is an obligation to carry out prescribed EDD measures when having any business interaction with these countries. It is typical that firms rely either on the output of their holistic customer risk assessment or a country risk assessment specific for payments to dictate when EDD measures are undertaken. It was identified in these 12 instances that when a firm's country risk assessment was not up to date or when their scoring methodology would not automatically raise the profile of the relationship and/or transaction to high risk, the firm could not confirm that mandatory EDD measures would be applied in all instances.

As a side note to the finding above, we note that of the 22 findings attributed to EDD, 12 were recorded due to the firm not applying some or all the prescriptive EDD measures to a business relationship or a transaction established in a HR3C (detailed further in the report). These findings, while similar, differ in the fact that the customer risk assessment should be a control used by firms to identify relationships with these high-risk jurisdictions, however, the prescriptive EDD is a control implemented to ensure that once identified, the legally defined due diligence is applied appropriately.

We noted on seven occasions that firms had identified customer-specific risks within their WFRA which had not then been considered within their customer risk assessment. As an example, a firm may consider within their WFRA, the risk of servicing a corporate customer with an overly complex ownership structure, however, if this is not then considered within a customer risk assessment, the firm cannot attest that they have implemented a suitable control to mitigate such a risk occurring.

On the three occasions where we identified that the output of a firm's customer risk assessment is not conducive to a robust risk-based approach, we note that one of following two issues were recorded:

- Too many or zero high risk customers,
- Too many or zero low risk customers.

In both of the above instances, we contend that regardless of the types of products and services a firm offers, or the jurisdictions they operate in, firms will have both a higher risk and lower risk subset of customers within their entire active portfolio. Without having oversight of the lowest risk and highest risk customers, it is not possible to ensure a risk-based approach has been applied. Without this, the firm may not allocate adequate resources to those customers or cases which require it most.

While a firm may attract higher risk customers by their nature, they will still have comparatively lower risk customers within their entire portfolio. Our recommendation is that firms set appropriate standard due diligence requirements according to their business model and customer base. If the business model and customer base is deemed to be inherently higher risk, the standard requirements should be more stringent. In addition, an appropriate EDD process should be developed to ensure that the higher risk subset of customers within the entire customer base are handled appropriately.

2. Whole Firm Risk Assessment (WFRA)

31 findings were identified in relation to firms' WFRAs. 14 were recorded as high impact and 17 were recorded as low impact. Of the 31 findings, 20 were found to be deficient based on the following four factors:

Finding Evidence	No. of Audits Affected
Detail within the WFRA is not considered granular enough	11
Firm has not developed a WFRA	4
Firm relies on an Enterprise Wide Risk Register - No AML specific risk assessment	3
No Risk Appetite Statement to accompany the WFRA	2

We note that 11 of the 20 issues identified above are attributed to the granularity of content firms have included within their WFRA. As detailed in regulation 18(3) of the MLRs, firms should consider both **'the size and nature of its business'** when deciding **'appropriate steps to identify and assess the risks of money laundering and terrorist financing to which its business is subject'**. As such, when reviewing a firm's WFRA, fscom is mindful that the impact of such a finding be considered in a similar vein.

It was determined by fscom that, on 11 occasions, the WFRAs reviewed during the audit process would not provide the reader (for example, the firm's senior management or board members) with sufficient oversight and/or insight into the firm's AML risk exposure, nor the effectiveness of their mitigating controls.

The issues within this finding would include the following:

- A determination that only high-level risks have been considered across the business,
- Not all key stakeholders have been involved in the identification and recording of risks,
- Risks are shown net of mitigating controls without showing or establishing underlying inherent risks,
- Where appropriate, data has not been utilised to give credence to the risk ratings attributed to both inherent and residual risk ratings, or
- There is no clear methodology regarding the assessment of the effectiveness of the mitigating controls.

With regards to a risk appetite statement (a finding attributed to two audits), fscom advises in all instances that a formal statement is compiled by the Board determining their appetite regarding their AML risk exposure. The firm's WFRA should then be read in conjunction with the statement to act as confirmation that they are operating within risk appetite, or to act as evidence that with their current controls environment, they are operating outside risk appetite and that a suitable action plan be implemented to return the business to a suitable operating model.

We note that four firms relied on an overarching Risk Register which consider risks across all business departments. While we accept that some AML and financial crime risks will be captured within a Risk Register, we recommend that all firms develop a standalone AML WFRA to ensure that they comply with regulation 18 of the MLRs. This finding is largely linked to the finding regarding a lack of granularity.

3. CDD (file testing)

31 findings were identified in relation to firms' CDD files, 7 of which were recorded as high impact and 24 of which were recorded as low impact. Of the 31 findings, 24 were found to be deficient based on the following four factors:

Finding Evidence	No. of Audits Affected
Source of Funds (SOF) and Source of Wealth (SOW) information has not been subject to sufficient scrutiny or corroboration	5
Insufficient verification for either the entity and/or relevant persons (UBOs, directors, authorised signers etc.)	8
Record keeping issues – missing supporting documentation (as required by Policy)	8
No evidence of screening included within the customer's CDD file (entity and/or relevant individuals)	3

As part of the audit process, fscom randomly selects no fewer than 20 customer files across multiple risk ratings, product offerings, and jurisdictions (where applicable). Files are reviewed to determine whether the due diligence collated and verified is in line with the relevant legislation as well as whether it complies with the firm's internal policies.

When informational gaps are identified regarding the firm's regulatory obligations, the impact of the finding is somewhat greater, while gaps identified regarding internal requirements to comply with the firm's policies may result in a slightly lower impact score.

A review of our previous audits reveals the following insights around where firms fall short:

8

In eight instances it was identified by fscom that the firm had insufficiently verified the information provided by the customer at onboarding or on an ongoing basis. On occasion, it may have been explained that verification measures were conducted via a desktop review. Nevertheless we advise that this is not certifiable if the verification information is not held within the customer's CDD file. We recommend that, where a source such as Companies House is used to verify information, the evidence be saved within the customer file. Should this information change throughout the business relationship, the customer file should be updated accordingly.

3

In three instances, confirmation of screening (against PEPs, sanctions, and adverse media lists) was not evidenced when customer files were reviewed. We recommend that firms can verify that customers are screened prior to their onboarding and that when an alert was raised, this was handled appropriately, in line with the firm's internal policies.

5

On five occasions, the firm had collected SOF and/or SOW information, however, it was identified under review that the information collected did not align with the customer's profile nor their proposed or actual transactional activity. Further, when the SOF/SOW provided was directly linked to customers requesting increased transactional limits, it was concluded that the information had not been sufficiently scrutinised or challenged.

4. PEPs, Sanctions, and Adverse Media

37 findings were identified in relation to firms' PEPs, sanctions, and adverse media screening, 10 of which were recorded as high impact and 27 of which were recorded as low impact. Of these findings, 29 were found to be deficient based on the following four factors:

Finding Evidence	No. of Audits Affected
PEP name(s) or sanctioned name(s) failed to generate an alert	14
No rationale attached to discounting false positives	5
Too infrequent or no ongoing monitoring	6
Fuzzy logic has not been adequately calibrated	4

As part of our review of a firm's PEPs, sanctions, and adverse screening process(es), we ask that the firm runs a test that we provide to determine the effectiveness of their screening tool(s). The test consists of:

- 15 known PEP individual names,
- 15 sanctioned entities and individuals, and
- 26 spelling variations of 1 PEP individual and 1 sanctioned entity or individual (13 variations for each).

As confirmed by the data above, during 14 audits, an alert was not generated on one or more occasions when either a PEP name or a sanctioned name (or both) were input into the screening tool. As such, there is an increased likelihood that the firm may provide their financial services to a PEP individual or a sanctioned person.

Firms have an obligation to not provide financial services to a sanctioned person or entity and as such, an occurrence of the above would be a breach of legislation. Regarding PEPs, a firm should have their own risk appetite, however, there is also a legal obligation to conduct prescriptive EDD measures before establishing a business relationship with a PEP. So if a firm is unaware of a PEP seeking to use or using their services, they may find themselves both in breach of the legislation, as well as non-compliant with their internal policy requirements.

To mitigate this risk, we recommend that firms conduct their own periodic testing of the screening tools they utilise to detect such activity. This should be included within their compliance monitoring plan and when deficiencies are recorded, the firm should contact their screening provider to present the evidence as well as seek an explanation.

The above issues are likely to occur when the fuzzy logic setting within a screening tool has not been calibrated at an optimum level. Often firms may adjust their fuzzy logic setting to reduce the number of alerts that are generated; however, we would recommend that in any instance where the fuzzy logic setting is adjusted, it is backed up by testing and data. Firms must ensure that by adjusting their fuzzy logic setting to reduce false positive alerts, they do not additionally eliminate false negatives.

When testing a firm's fuzzy logic setting, our intention is to provide relevant feedback when spelling variations which we contend the firm may wish to have oversight of do not generate an alert for a potential match. Examples may include:

- One letter changed,
- Two letters changed,
- One letter removed or added, and
- First name and surname stuck together.

Finally, when reviewing a firm's investigations and escalations procedures, it was identified that five firms did not require that analysts attach commentary or rationale to the discounting of screening alerts deemed to be false positives. We contend that in such instances, the lack of a robust audit trail will not allow for quality assurance (QA) or quality control (QC) to be carried out to ensure false positives are discounted in line with the firm's internal policies.

5. Compliance Monitoring

32 findings were identified in relation to firms' compliance monitoring, 11 of which were recorded as high impact and 21 as low impact. Just four factors caused deficiencies in 28 of these filings:

Finding Evidence	No. of Audits Affected
No compliance monitoring plan has been developed	13
A compliance monitoring plan has been developed but it is not yet operational	8
While ad hoc testing is carried out, it has not been formalised and the output is not recorded	5
The firm is not up to date with their compliance monitoring plan	2

Regulation 19(3)(e) states that **'The policies, controls and procedures referred to in paragraph (1) must include the monitoring and management of compliance with, and internal communication of, such policies, controls and procedures'.** Paragraph 1 refers to policies, controls and procedures which must be established to mitigate and effectively manage the risks of money laundering and terrorist financing identified in any risk assessment undertaken by the firm (with regards to regulation 18).

As such, we consider that a firm's compliance monitoring plan should take into account the size and nature of the business. This is similar to our recommendation for a firm's WFRA. We further suggest that a robust monitoring plan should work in conjunction with a WFRA in that the policies, controls, and procedures detailed within should be monitored on a periodic basis dependent on the risk(s) they are tasked with mitigating as well as the assessment of their effectiveness.

Based on the data above, we were not able to review a firm's monitoring plan due to there not being one developed on 13 occasions, or a developed plan having not been implemented in eight audits.

As detailed above, five firms were conducting ad hoc testing. However, this was generally carried out when resource allowed, and there was no formal output recorded by way of an audit trail. As such, on these occasions, we were not able to evidence in the first instance that testing had been undertaken, nor in the second instance that when issues were identified, how these had been addressed.

Two findings arose due to firms not being up to date with their compliance monitoring plan. We recommend that in developing a plan, while the firm should consider both their size and nature, as well as their WFRA, they should have sufficient resource to ensure the plan can be carried out as anticipated and that where issues are identified, suitable action plans can be implemented and tracked to completion.

Review and testing areas with between 20 and 25 findings

While the five review and testing areas listed above had over 30 findings identified across the 57 audits, we note that the categories of EDD as well as periodic and event driven reviews both had over 20 findings identified, with 22 and 23 findings respectively. We further note that EDD had the second highest number of high impact findings with 12. Only WFRA had more high impact issues identified with a total of 14. Further, the periodic and event driven review category had 10 high impact findings identified, the fourth highest along with the PEPs, sanctions, and adverse media category.

Across the next two sections, the report will focus on issues identified within both the EDD and periodic and event driven review categories, with particular attention aimed at these high impact issues and what caused them.

1. EDD

22 issues were identified in the EDD category, 12 of which were rated as having a high impact for the firm and 10 rated as having a low impact. These findings had three deficiencies in common:

Finding Evidence	No. of Audits Affected
The firm has not applied or would not likely apply all prescribed EDD measures to HR3Cs	12
The firm's policies do not mandate that both SOF and SOW information is collected for PEP individuals	2
The firm does not have a formal EDD procedure	8

Conducting audits throughout the period analysed in this report, it was evident that firms had somewhat overlooked their legal obligation to monitor for customers and transactions established in HR3Cs. Further, that the HR3C list, particularly in the UK, is subject to change quite regularly and firms were often not up to date in their own assessments.

When prescribed EDD measures are dictated for PEP relationships (regulation 35) and correspondent relationships (regulation 34), regulation 33(1)(b) of the MLRs is clear about what is required for firms seeking to have **'any business relationship with a person established in a high risk third country or in relation to any relevant transaction where either of the parties to the transaction is established in a high risk third country'.**

As set out in regulation 33(3A):

> ‘The enhanced due diligence measures taken by a relevant person for the purpose of paragraph (1)(b) must include —
>
> (a) obtaining additional information on the customer and on the customer’s beneficial owner;
>
> (b) obtaining additional information on the intended nature of the business relationship;
>
> (c) obtaining information on the source of funds and source of wealth of the customer and of the customer’s beneficial owner;
>
> (d) obtaining information on the reasons for the transactions;
>
> (e) obtaining the approval of senior management for establishing or continuing the business relationship;
>
> (f) conducting enhanced monitoring of the business relationship by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.’

Regarding the 12 instances where the above had not been (or would not likely be) applied, the rating assigned to these findings was generally high impact. There were occasions where a firm had no dealings with HR3Cs and as such, while their policies and procedures were deemed to be deficient, the impact of the finding was diminished based on their customer base.

It was a regular theme that firms were applying some of the measures as defined in regulation 33(3A), however, not all of them. We found that the most regular failings were regarding senior management sign off and obtaining information on the source of wealth on the customer and the customer’s beneficial owner (where applicable).

We recommend that firms are mindful of these specific EDD obligations when entering these relationships.

On eight occasions, it was determined that the firm’s EDD procedure was wholly ad hoc and there was no formalisation of what should be carried out when certain high risk scenarios present themselves. While a bespoke model may work for certain firms and on occasion, generally a procedure such as this is not scalable and as such, we would recommend the firm sets several specific EDD measures for the more likely high risk scenarios, for example, specific measures when a customer is labelled as high risk due to their industry type or their expected payment locations or transfer volumes.

In addition to the above, the firm may, following a review by a relevant employee, dictate several other requirements based on the individual nature of each high risk case. This procedure would ensure that on-boarding analysts can, based on the output of a customer risk assessment, gather some (or all) necessary EDD requirements prior to escalating the case to a relevant senior employee.

2. Periodic and Event Driven Reviews

23 issues were identified in the periodic and event-driven reviews category, ten of which were rated as having a high impact for the firm and 13 rated as having a low impact. Of the 23 findings, 17 were deemed to be deficient based on the following factors:

Finding Evidence	No. of Audits Affected
The firm has a backlog of customer accounts which have not been subject to a periodic review	10
The firm does not have a formal periodic review procedure for all customers	7

As the data confirms, the primary issue firms are facing with regards to periodically reviewing their customer base is remaining up to date with the workload. 10 out of the 57 firms reviewed had a backlog of some description with varying numbers of customers overdue as well as varying periods over which a backlog has accumulated.

While limited resource is generally the primary reason for a backlog developing, we reviewed cases where firms were beginning their customer reviews on the date they became overdue. We noted that, on occasion, a review of a customer account (generally a corporate account) could take as long as several months, depending on the customer's response to requests for information. As such, a firm should consider the likely length of a review and update their policy to begin their customer reviews ahead of time to increase the likelihood that reviews are signed off prior to or on the day the customer account becomes overdue.

On seven occasions, we reviewed firms which had not yet implemented a periodic review procedure. The reasons for this included:

- They had only recently become operational, and no customers had been onboarded long enough to warrant a review,
- The firm placed a reliance on their event driven reviews to ensure oversight of their customer base, and
- The firm only periodically reviewed their higher risk customers and relied on their event driven reviews to monitor their low and medium risk customers.

For firms that had only recently become operational, we recommend that their policies clearly state how often reviews should take place, and that ahead of due dates arriving, the firm should determine who will be tasked with undertaking reviews, and what a review will entail.

For firms relying on their event-driven reviews, there was often little evidence that the firm's entire customer base would be captured by such events, and therefore the firm could not attest that all their customers would be subject to an account review during the business relationship.

While our reviews of these firms' processes highlighted deficiencies in their substitution of a periodic review for a reliance on event-driven triggers, we are mindful that this approach is being more widely considered for certain types of firms with certain types of customers. We therefore recommend that these firms consult the guidance issued by the Wolfsberg Group which provides information regarding 'shifting to a targeted, disciplined approach to on-going due diligence by refreshing customer data on a trigger (rather than periodic) basis, dedicating resources effectively to priority risks in real-time'.

Wolfsberg Guidance on Digital Customer Lifecycle Management (wolfsberg-principles.com)

In particular, firms should be aware of and be able to implement the preconditions stated by Wolfsberg that would support such an approach.

Review and testing areas with between 10 and 20 findings

Stepping back and taking a wider review of the data from our audits, five review and testing areas stand out for recording between 10 and 20 findings. They are:

SARs	17 findings
AML Training	17 findings
Transaction Monitoring	17 findings
MLRO Reporting and MI	18 findings
AML Policies and Procedures	12 findings

We will now dive further into each area to focus on the issues identified and how firms can mitigate them:

1. SARs

Regarding the 17 findings attributed to SARs (7 high impact and 10 low impact), we recorded ten separate issues. The four most common are:

Finding Evidence	No. of Audits Affected
The firm has a material backlog of unactioned internal SARs	3
The firm has not implemented a formal internal reporting procedure	3
The firm does not require that rationale is attached when a customer is offboarded due to potentially suspicious transactional behaviour, but an external SAR is not filed	2
The firm has not developed a centralised log to track all internally reported suspicions	3

As set forth in the Proceeds of Crime Act 2002 (PoCA), a nominated officer in the regulated sector commits an offence if he **'does not make the required disclosure to a person authorised for the purposes of this Part by the Director General of the National Crime Agency as soon as is practicable after the information or other matter mentioned in subsection (3) comes to him'**. While no timeframe is mentioned within the Act, it was determined that during three audits, the materiality of the backlog of unactioned internal SARs had overrun a period which could reasonably be described as 'as soon as practicable'.

In all three instances, the firms had seen an increase in activity which had led to a rise in internal reports. At the point in time of the three respective audits, additional resource had not been employed to cope with the increased number of internal reports. We recommend that MI should be generated and used to periodically track the performance of the business, the number of transactions being processed, and the number of alerts being generated as these factors are likely to correlate with the number of internal reports routinely received. Based on the relevant MI, potential resource issues can be addressed prior to material backlogs emerging.

In three separate instances, firms had yet to formalise their internal reporting procedure. In most cases, staff members could raise suspicions in many forms (verbally, through Slack channels, or via email) to many employees within the compliance function. We recommend ensuring a robust reporting process and maintaining clear audit trails. Firms should determine formal reporting lines and relevant employees responsible for conducting subsequent investigations.

The further five findings listed in the table above (along with the remaining issues not listed) relate to the way in which a firm logs, tracks, monitors, and closes off any internal investigations or external SARs. It was noted on several occasions that some internal reports were held within numerous depositories, such as email inboxes, Slack chats, or saved in the customer's file on a Customer Relationship Management (CRM) database. fscom recommends ensuring a robust audit trail and acquiring an overview of customers consistently flagged internally as displaying potentially suspicious behaviour. All reports should be recorded within a centralised SAR log.

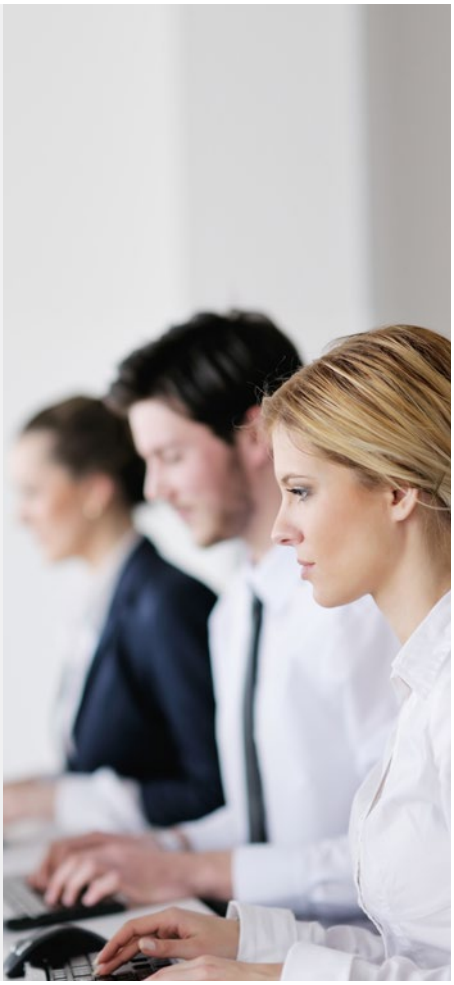
2. AML Training

17 issues were identified in the AML training category, four of which were rated as having a high impact for the firm and 13 as low impact. Of the 17 findings, 12 were deemed to be deficient based on the following factors:

Finding Evidence	No. of Audits Affected
The firm's employees are not up to date with their AML training obligations	6
The AML training course does not have a supplementary assessment to verify employee understanding	4
The firm does not require that training is updated periodically, for example, annually	2

When reviewing a firm's AML training regime, the focus of the side-by-side walkthrough is to establish and verify the following:

- Are new starters subject to AML training? If so, are there any roles which are exempt?
- How soon before this training must be completed?
- Can a new starter (particularly in a customer-facing role) commence their role prior to the completion of their AML Training?
- How is the AML training delivered and who by?
- Who is responsible for deciding on the content and ensuring it remains up to date?
- How is the progress and completion of training recorded and monitored?
- Are staff required to complete an annual refresher AML training course? If so, are there any roles which are exempt?
- How is a staff member's understanding of the AML training content verified?



We would expect that the firm has an AML training policy in place which considers the questions above. Our side by side walkthrough then acts as verification on whether the policy has been followed.

The most identified issue during our review of firms' AML training programs is where employees are not staying up to date with their training obligations. As detailed above, on six occasions, it was identified that employees were overdue the completion of their training. Deadlines for the completion of AML training should be set out by firms within their training policy. Thereafter, a relevant department or individual should be tasked with the responsibility of ensuring these deadlines are met, recorded, and monitored, as well as shared with senior management in the form of MI.

We observed that firms generally set clear deadlines and assigned relevant employees to ensure these deadlines are met. However, firms often did not have a clear procedure when these deadlines were routinely missed. As the completion of AML training by relevant employees is a regulatory obligation, firms must have in place robust procedures to appropriately manage employees who fail to complete courses within the set timeframes. While email reminders may suffice in the short term, firms must consider further escalation procedures, including even the temporary suspension of employees who continue to fail to comply.

In four instances, we noted that firms did not assess whether their employees had understood the information that had been delivered. As more firms have moved to an online-based AML training programme, we would recommend that any training course provided is supplemented by an assessment in which employees must achieve a suitable score to be deemed to have passed. Results of the assessment should be recorded within the training log.

Firms should outline within their training policy, the necessary steps to be taken when employees fail to achieve a pass mark in an AML training assessment.

On two occasions, we noted that firms did not provide refresher training to employees. Generally, industry standard is that refresher training is provided firm-wide annually. However, at a minimum, firms should consider the following information from the JMLSG guidance when implementing a refresher training procedure:

'The firm's approach to training should be built around ensuring that the content and frequency of training reflects the risk assessment of the products and services of the firm and the specific role of the individual.' JMLSG Guidance, 7.22

3. Transaction Monitoring

17 issues were identified in the transaction monitoring category, three of which were rated as having a high impact for the firm and 14 as having a low impact. Of the 17 findings, 11 were deemed to be deficient based on the following four factors:

Finding Evidence	No. of Audits Affected
The firm does not require that alerts deemed not to be suspicious have rationale attached	2
The initial investigation process requires enhancement – Analysts do not in all instances review the customer's KYC information and/or their transactional history	2
Post transaction alerts are not subject to a timely enough review in all instances	2
The firm has developed a material backlog in transaction monitoring alerts which have not been reviewed and actioned	5

As evidenced above, the most common issue identified with a firm's transaction monitoring process was that material backlogs had developed. The word 'material' is key to this finding as we understand that at certain times of the year, or due to unforeseen spikes in activity, minor backlogs may emerge, however, we would consider a material backlog to be one which is borne out of too many alerts being consistently raised without the resource to ensure they are reviewed within a timely manner.

We recommend that firms rely on historical data to ensure they are prepared for likely spikes in activity. Additionally, we recommend that firms conduct testing of new rules which they wish to implement and analyse the additional workload which is likely to emerge when the new rules are introduced into their live rulesets.

We further recommend that firms set out within their policies clearly defined SLAs for the review of transaction monitoring alerts. Firms should set these SLAs on a priority basis. For example, alerts for high risk customers, or due to the involvement of high risk jurisdictions, may require a more urgent review.

We noted on four occasions that analysts were deemed not to be carrying out their reviews of alerts to a high enough standard. On two occasions, the issue was that their reasoning for discounting alerts as false positives was not documented and attached to the case. As such, there is no capability for quality assurance checks to be conducted to ensure that a manager is satisfied a review was conducted according to the firm's procedure and that they agree with the final decision and reasoning. Further, as part of the audit process, we would look to review several transactions which have alerted and, without a robust audit trail, it is difficult to attest that alerts have been handled appropriately.

On two further occasions, it was identified that the analysts were not using relevant customer information when conducting their reviews of transaction alerts, for example, the customer's prior transactional activity, and/or their KYC information. When reviewing transaction alerts, there are many instances when suspicion can only be determined based on the customer who has generated the alert. What is suspicious for one customer may be normal behaviour for another, however, without reviewing their KYC information, or their prior activity, Analysts would more likely be making assumptions, rather than making an informed determination.

4. MLRO Reporting and MI

18 issues were identified in the MLRO Reporting and MI category, six of which were rated as having a high impact for the firm and 12 rated as having a low impact. Of the 18 findings, 16 were deemed to be deficient based on the following three factors:

Finding Evidence	No. of Audits Affected
No (or insufficient) formalised MI procedure	7
No (or overdue) MLRO report	7
The firm's MLRO additionally holds another position of seniority within the company	2

During the MI walkthrough, we typically review the type of information which is escalated up and across the business to inform key decision makers and senior management regarding the firm's AML and financial crime framework as well as the effectiveness of the mitigating controls implemented to ensure the business operates within their defined risk appetite.

Six key questions your auditor will want to know

We will review the above based on the following:

- What AML (and other financial crime) specific information is routinely featured within an MI pack?
- Who is responsible for collating the information and data?
- How is the information and data compiled?
- To whom is this MI presented and how often?
- Are these presentations recorded and minuted?
- Has any MI brought about changes within the business? If so, how has this been recorded and tracked?

While the answers to several of the questions above will be subject to change from firm to firm based on their size and nature, we would generally anticipate that the type of information which is presented as part of an MI pack would be consistent. We refer firms to section 2.2.2 of the FCA's Financial Crime Guide which sets out what would be considered sufficient information:

'MI should provide senior management with sufficient information to understand the financial crime risks to which their firm is exposed. This will help senior management effectively manage those risks and adhere to the firm's own risk appetite. MI should be provided regularly and ad hoc, as risk dictates.

Examples of financial crime MI include:

- an overview of the financial crime risks to which the firm is exposed, including information about emerging risks and any changes to the firm's risk assessment
- legal and regulatory developments and the impact these have on the firm's approach
- an overview of the effectiveness of the firm's financial crime systems and controls
- an overview of staff expenses, gifts and hospitality and charitable donations, including claims that were rejected, and
- relevant information about individual business relationships, for example:
  - the number and nature of new business relationships, in particular those that are high risk
  - the number and nature of business relationships that were terminated due to financial crime concerns
  - the number of transaction monitoring alerts
  - details of any true sanction hits, and
  - information about suspicious activity reports considered or submitted, where this is relevant.

MI may come from more than one source, for example, the compliance department, internal audit, the MLRO or the nominated officer.

On seven occasions, it was identified that the firm was overdue their presentation of an annual MLRO Report to the Board. In some instances, with robust MI procedures in place, a firm may conclude that an annual report is not necessary. As there is only an obligation to report to senior management and the Board no less than annually, this would be an acceptable process if the MI reports succeed in providing a holistic overview of the firm's AML framework, the regulatory landscape in which they operate, any issues identified, and allows for a financial crime roadmap to be developed and tracked to completion.

Most firms would, however, conclude that an MLRO report, in addition to periodic MI, provides the MLRO an opportunity to present a detailed analysis across a full year's worth of data and set out a priority based action plan to be approved and signed off by the board. The plan may address resource issues, present audit findings, update them on AML training completion rates, and discuss budgetary requirements for the implementation of new controls and/or procedures where weaknesses have been identified or regulatory changes have occurred.

Based on the data above, we identified seven instances when an MLRO report was overdue its annual presentation to the board. As such, we concluded that the firm's board and senior management did not have adequate oversight of the firm's AML and financial crime framework nor any issues which may have needed to be addressed.

Twice, we identified that the MLRO additionally held another position of seniority within the firm, which generates a potential conflict of interest for the firm and could mean that the MLRO lacks a sufficient level of independence. It may also be argued that fulfilling two roles would not allow the MLRO enough time to ensure their role as a reporting officer is afforded enough of their attention.

5. AML Policies and Procedures

12 issues were identified in the AML policies and procedures category, two of which were rated as having a high impact for the firm and 10 rated as having a low impact. Of the 12 findings, 10 were deemed to be deficient based on the following three factors:

Finding Evidence	No. of Audits Affected
The firm's AML policies and procedures are overdue an annual review (as per the firm's compliance monitoring plan)	4
The firm's AML policies and procedures are not reflective of the size and nature of the firm	2
Discrepancies were identified between the information contained in the AML policies and procedures and the processes reviewed during the audit	4

As required by the MLRs:

'A relevant person must— (a) establish and maintain policies, controls and procedures to mitigate and manage effectively the risks of money laundering and terrorist financing identified in any risk assessment undertaken by the relevant person under regulation 18(1); (b) regularly review and update the policies, controls and procedures established under sub-paragraph (a)'

We see as industry standard and recommend as best practice that a firm's AML policies and procedures are subject to a review no less than annually. However, we note that when there are relevant changes, these reviews should be brought forward to reflect them.

Even when there are no material changes in the firm's AML framework, we recommend an annual review is conducted and its occurrence signed off or detailed within a version control section of the document. The reviewer, date of the review, and any changes should be captured.

Further, we recommend that policy and procedure reviews are documented and tracked within a firm's compliance monitoring plan. This will ensure further that reviews are carried out within internally developed timeframes. The output of these reviews can then be more readily available to include within MI packs for presentation to senior management.

As detailed in the table above, it was identified on four occasions that a firm's policies and procedures had not been subject to an annual review.

On a further four occasions, we noted that the policies and procedures displayed discrepancies between what is documented in writing and what occurs day to day. Discrepancies were generally identified when firms failed to review and update their policies either annually, or when significant changes occur, for example, the implementation of a new screening provider, or an update to their EDD requirements.

Finally, we noted in two instances that a firm's policies and procedures were not reflective of both the size and nature of that firm. A firm should ensure in all instances that their policies and procedures assist them in mitigating and managing the money laundering and terrorist financing risks presented to them. Firms of a certain size, offering certain services to certain client types in certain jurisdictions, must be mindful of the specific risks to which they are exposed, and ensure their policies and procedures achieve that which is required by law.

Review and testing areas with less than 5 findings

1 – CDD (regarding the firm's policy)

The data confirms that CDD (regarding the firm's policy) accounted for the least number of findings with only six identified across 57 audits – and only three of these were recorded as high impact. However, we should be mindful that on 31 occasions, issues were recorded regarding the firm's application of their CDD policy (during the CDD file testing). As such, we conclude that while firms have developed relatively robust policies and procedures regarding CDD in theory, this is not always backed up in practice.

The six findings were deemed to be deficient based on three factors:

Finding Evidence	No. of Audits Affected
The firm's CDD policy does not account for the reporting of UBO discrepancies to Companies House	3
The firm has not implemented a formalised customer account dormancy policy	2
The firm has not implemented a procedure for the deletion of customer CDD files	1

'The relevant person must report to the registrar any discrepancy the relevant person finds between information relating to the beneficial ownership of the customer—

(a) which the relevant person collects under paragraph (1); and

(b) which otherwise becomes available to the relevant person in the course of carrying out its duties under these Regulations when establishing a business relationship with the customer.' MLRs, Regulation 30A(2)

With the introduction of the 5th Anti-Money Laundering Directive (5AMLD), which came into force on 10th January 2020, firms have an obligation to report discrepancies in beneficial ownership information if any are identified at onboarding or on an ongoing basis. On three occasions, it was identified by fscom that firms had not considered this within their policy, nor had they implemented procedures for the reporting which would need to occur upon such a discovery.

We note that a robust CDD policy should recognise the transposition of this obligation under 5AMLD, and additionally, should indicate who is to be responsible for the reporting of discrepancies, and how this activity is to be carried out and be recorded, monitored, and reported internally. For the reporting of beneficial ownership discrepancies, we provide the following link:

Report a discrepancy about a beneficial owner on the PSC register - GOV.UK (www.gov.uk)

On two occasions, it was noted that the firm would consider accounts dormant should they not have used the firm's services for a certain period but the firm had not implemented a formal procedure detailing how these customer accounts should be reviewed should the customer attempt to carry out a future transaction. This presents a risk because, on both occasions, an account falling into dormancy would subsequently become exempt from the periodic review process, however, where a clear dormancy policy has not been established, the robustness of this control is diminished.

While we accept that customers should be labelled as dormant should they cease using the firm's services for a defined period, the firm should ensure that should this customer wish to resume availing of the firm's services, a robust procedure for an account review is established and formalised in policy. This may mirror the firm's periodic review process or may be developed on a case-by-case basis, and firms should always ensure that they are servicing their customer based on current CDD information.

Summary

Financial crime becomes more prevalent with every passing year, as criminals acquire increasingly sophisticated means of laundering money and financing terrorism. According to the International Compliance Association, financial crime now accounts for 3.6% of global GDP. It also drives global corruption and inequality which has devastating consequences for many millions of people around the world. The risks faced by financial services firms are also growing, while these firms also face pressures on their compliance resources.

In this report, we dove deep into the data from 57 audits carried out by fscom over the last year to identify where firms tend to have deficiencies in their AML controls. We then pulled back and looked at the best practices firms have implemented to address these deficiencies and mitigate the ever-growing risks.

When we reflect on our experience across all the reviews analysed in this report, a picture emerges of firms who tend to focus on the bigger picture – establishing the key components of a robust AML/CTF framework and procedures – or the detail – specific, perhaps to new or unfamiliar legal and regulatory obligations. But often, firms do not look at both the bigger picture and the detail. We very frequently find that a firm with a well-developed overall framework carries gaps when it comes to detailed obligations. Or in other cases we find firms with extensive rules and procedures that require detailed adherence to specific regulatory points but where the major structures of the framework are not robust enough to properly make this exactitude, reliable or effective.

This report should give you and your firm indicators of where you might be doing well, and where you might have more to do. Given the growing risk of financial crime, these indicators are more important than ever before. We would be glad to discuss what implications you think this report has for your compliance process in more detail, and how fscom can help with this important process. Don’t hesitate to contact us.

About fscom (FSCom Limited)

fscom is one of the leading specialist consulting firms providing governance, risk, and compliance solutions to financial services institutions in the UK and Ireland.

fscom is a firm of deep domain experts who specialise in the payments and e-money, crypto, FX broking, fund and asset management and consumer credit sectors.

The senior team is a unique mix of experienced consultants, ex-regulators, ex-bankers and former in-house compliance experts who hold senior positions with leading compliance related industry associations and provide clients with in-depth regulatory insight and industry best practice in all areas of financial services regulation to include authorisation, audit, financial crime, cyber security, and regulatory due diligence.

Our Experts

Philip Creed
Director
Financial Crime
philip.creed@fscom.co

Richard Dunlop
Senior Compliance Associate,
Financial Crime
richard.dunlop@fscom.co

fscom
Expertise that adds value.

Let's start a conversation.

Have a compliance question?

+44 (0) 28 9042 5451

info@fscom.co

fscom.co