Dubai Financial Services Authority

ANNUAL ANTI-MONEY LAUNDERING RETURN

ANALYSIS AND GUIDANCE

Issued April 2015

Contents

Executive Summary

Background

In July 2013, the Dubai Financial Services Authority's (DFSA) new Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF) and Sanctions Module of the DFSA Rulebook (the AML Module) came into force. The key drivers for such changes were to:

- bring DFSA's AML[1] regime into line with the revised 2012 Financial Action Task Force (FATF) recommendations on combating money laundering and terrorist financing; and

- consolidate into one Module the DFSA's AML requirements for Authorised Firms (AFs), Authorised Market Institutions(AMIs), Designated Non-Financial Businesses and Professionals (DNFBPs) and Auditors, collectively referred to as "Relevant Persons".[2]

One of the enhancements to the AML Module was the introduction of the Annual AML Return (AML Return) which replaced the Money Laundering Reporting Officer (MLRO) Report. The new AML Return has been designed specifically to provide the DFSA with targeted and specific information on a Relevant Person's AML systems and controls.

The findings of this report should be considered by all Firms in reviewing and implementing their ongoing AML programs. The findings are based on an analysis of the 2014 AML Returns; they should not be viewed as exhaustive but as guidance to be applied where relevant. As with any new reporting requirements, the DFSA anticipated that the first round of Annual Returns would present a number of improvement opportunities. For example, some Firms failed to understand or misinterpreted the questions being asked in the AML Return. Many Firms also failed to consider the specific rules which were referenced in the questions.

In assessing these first submissions, the DFSA deliberately adopted a more lenient approach in feedback and criticism. Moving forward however given the guidance and feedback provided during the process and this report, the DFSA will have higher expectations for improvements in the timeliness and quality of future submissions.

The overall structure of the AML Return has been designed to mirror the relevant provisions in the AML Module. Relevant Persons are required to provide both narrative and practical examples displaying how it complies with its obligations under the AML Module. The AML Return also seeks specific, qualitative data, for example, the number of particular clients or Political Exposed Persons (PEPs). Such data will assist the DFSA in better understanding the AML landscape and risks in the Dubai International Financial Centre (DIFC).

As importantly, the process of preparing an AML Return provides an opportunity for a Relevant Person to conduct a self-assessment, which should assist in highlighting any key risk areas and improvement opportunities. However, we remind Relevant Persons that the AML Return is not a substitute for notifying the DFSA of relevant events as and when they happen.[3]

---

[1] Any reference in this report to the "AML requirements/risks/obligations" should be read as a reference to the DFSA's AML, Counter-Terrorist Financing (CTF) and sanctions regime.

[2] Any reference to a "Firm" should be read as a reference to a Relevant Person.

[3] See AML Rules 14.3.1 and 14.6.1.

Summary of Key Findings and Observations

Senior Management and Sign off	• a significant number of Firms did not properly identify their senior management and/or failed to obtain their acknowledgement and sign off. • acknowledgement and sign off is one way that senior management is able to evidence its oversight and responsibility for the Firm's compliance with its AML obligations.
Assessment of Business AML Risk	• the quality of the documentation of a Firm's AML risk assessment varied from very good to very poor. • areas of improvements include the need for Firms to tailor their assessments specifically to their business, and obtain buy-in from all areas of the Firm including senior management, compliance and business lines.
Assessment of Customer AML Risk	• most Firms displayed a good grasp of the factors that should be taken into consideration when assessing the specific risks posed by customers. • some customer risk assessments placed too great an emphasis on the country or jurisdiction from which a customer was from, without considering the associated product or service risk. • the assessment of customer risk should be appropriately documented so that all information known of the customer for example by their relationship manager can be collectively shared within the organisation.
Customer Due Diligence (CDD)	• most Firms were able to document and evidence the CDD processes undertaken when on-boarding new customers and such steps were generally well articulated and clear. • areas of improvement include the requirement to conduct ongoing CDD such as transaction monitoring. • many Firms appeared to rely on the fact that transactions were booked overseas to not monitor transactions from the DIFC.
Reliance and Outsourcing	• a significant number of Firms misinterpreted questions in this section and failed to appreciate the difference between placing reliance on, or outsourcing CDD measures to a third party[4], from using a third party information vendor or screening software.

[4] Chapter 8 of AML Module

Suspicious Activity Reports (SAR)	• 54 internal notifications relating to suspicious activities, and 50 external SARs were lodged by Firms • The trigger for submitting an internal notification should be as expansive as possible with the MLRO then acting as a second stage and ultimately deciding if an external SAR should be lodged. Accordingly, the DFSA expected that the number of internal notifications would be significantly higher than the number of external SARs.

The overall findings from the analysis of the 2014 AML Returns, confirms and supports the DFSA's continued focus on AML related risks. The above findings will assist the DFSA in preparing for any national AML risk assessment undertaken pursuant to the 2012 FATF Recommendations. Additionally, they will also assist in the scoping and setting of our AML regulatory priorities. This may include conducting a specific Financial Crime thematic review which may focus on:

- **Risk-Based Approach** - ensuring risk-based assessments undertaken are objective and proportionate, based on reasonable grounds, properly documented, and reviewed and updated at appropriate intervals;[5]
- **Ongoing CDD** - assessing the appropriateness and quality of ongoing CDD, in particular ongoing risk reviews and transactions monitoring;[6] and
- **Suspicious Activity Reporting** - improving the internal escalation process for the notification of suspicious activities and transactions and enhancing the quality of external SARs submitted to the Anti-Money Laundering Suspicious Cases Unit (AMLSCU) of the Central Bank of UAE.

[5] Chapter 4 of the AML Module

[6] Rule 7.6.1 of AML Module

Introduction

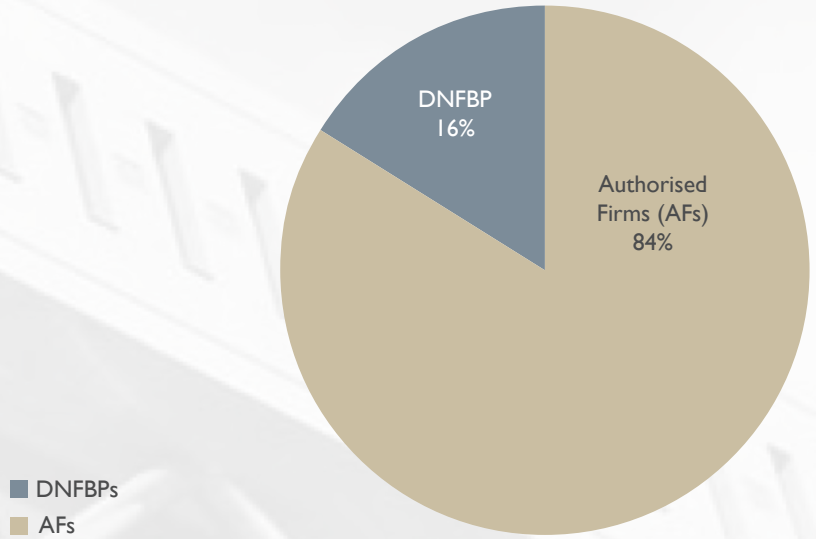
The findings of this report resulted from the analysis of AML Returns submitted during 2014. The review was designed to make high level and general observations on how Firms approach AML risks in the DIFC. While individual submissions have been analysed, this report is published on a no names basis and should be considered as generic guidance. The review therefore, does not necessarily contain any specific follow-up actions undertaken by the DFSA.

Firms should contact their DFSA relationship manager, if one has been assigned or via the DFSA contact portal if they have any questions.

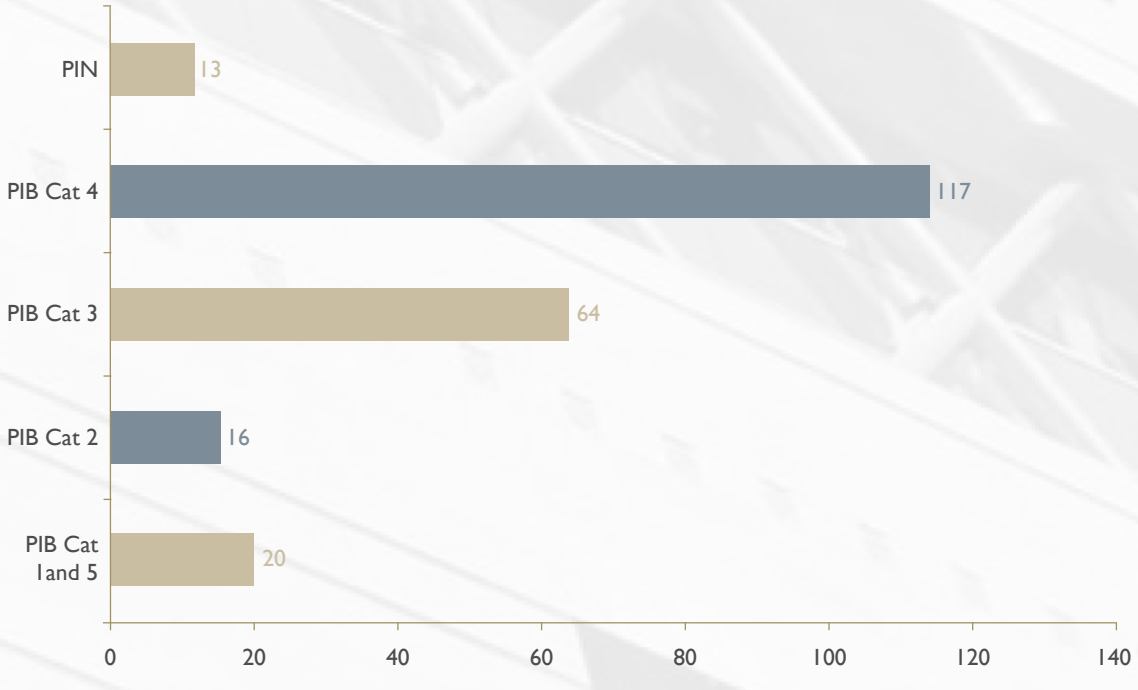
In terms of overall statistics, the following is noted:

- 279 AML Returns were considered for the purposes of this review;
- 233 of these were from AFs and 46 of these were from DNFBP;
- 90% of the AML Returns were received on time, or as result of an extension of time being agreed with the DFSA;
- 37% of submissions required no or minimal follow-up from the DFSA;
- 63% of submissions required follow-up including requests for clarification, requests to provide further information or requests to correct clearly erroneous information; and
- Total sample split by Firm and prudential category is illustrated overleaf:

Total Sample Size = 279 Firms



Breakdown of Authorised Firms in Review



General Findings

The AML Return was designed to be read and answered in conjunction with the AML Module. For ease of reference, the various components of the AML Return make reference to the relevant AML Rule. These rules should be consulted prior to answering each section to ensure that answers are relevant and in context.

Overall, our analysis identified the following general issues regarding Firms understanding of and response to some of the questions in the AML Return. In particular :

- some Firms misinterpreted or did not understand the questions being asked. For example, **Section C1**[7] asks for the listing of *"individuals forming the senior management of the firm."* The term senior management is a defined term in the AML Module and in these instances respondents simply named the SEO and Compliance Officer, omitting other members of senior management;

- some Firms did not answer the questions as required which resulted in insufficient details to assess the answer. For example, in **Section D3**, Firms are asked to *"state the date or dates when the last risk assessment was carried out on the adequacy of its AML systems and controls."* Some Firms failed to provide a date or provided vague answers such as "routinely";

- many of the questions asked in the AML Return are multi-facetted and require more than one answer. Using **Section D3** as an example, it asks Firms *"to provide or attach a summary of the findings of this assessment."* Often this was not provided and no explanation provided for the failure to answer.

Lessons Learnt

In order to improve the quality of future AML Returns, Firms should take into consideration the following:

- read and completely understand the context of the question before attempting to answer it;

- consult with the AML Module and its glossary and be conscious of the use of defined terms;

- double check that the answer is complete and includes a response to each sub element, including why the Firm thinks an answer is not applicable or unanswerable; and

- provide specific numbers and dates, or an explanation as to why these cannot be provided when asked for specific information.

[7] All Sections refered to in this Report are base on the most recent Annual AML Return - AML/VER3/03-15.

Specific Findings

Senior Management Responsibility and Sign off (Section C1 & C7)

The DFSA believes that a significant influence on a Firm's compliance culture is set by the "tone at the top". To emphasise this, every individual who forms part of a Firm's senior management, as defined in the AML Module[8], is responsible for a Firm's compliance with its AML obligations. In carrying out their responsibilities every member of the Firms senior management must exercise due skill, care and diligence.

As such the following should be noted:

- where the AML Return seeks the names of all individuals forming the senior management of the Firm, that the named individuals **(Section C1)** meet the definition of senior management contained in the AML Module;

- the DFSA also requires that the AML Return be acknowledged and signed off by every member of senior management. This ensures that those who are being held accountable for AML compliance within the Firm are aware of the contents of the AML Return; and

- in acknowledging and signing off on the AML Return, the DFSA values substance over form. Should senior management wish to acknowledge and signoff the contents of the AML Return via board resolution or other mechanism, evidence of such should be attached to the AML Return.

It was encouraging to see many responses which displayed that senior management has a strong involvement in AML related decisions such as:

- actively participating in risk assessment discussions of the AML risks faced by the business, including new products;

- AML being a standing agenda item on Board meetings; and

- Board approval of enhancement opportunities identified during the completion of the AML Return.

Money Laundering Reporting Officer (MLRO) (Section C2-6)

The primary support mechanism to senior management in ensuring compliance with AML requirements is a Firm's MLRO. The MLRO has oversight over day to day operations for AML compliance and acts as point of contact for employees by receiving internal suspicious activity notifications. Further the MLRO acts as a point of contact for the DFSA and the AMLSCU.

The AML Return responses provided the DFSA with a snapshot of MLROs in the DIFC and will also allow the DFSA to monitor any changes, year on year. Some observations in relation to MLROs include:

[8] As defined in Chapter 3 AML Module: Glossary for AML.

- nearly all Firms had a good grasp on the importance of the MLRO and were able to articulate their duties clearly in **Section C4;**

- approximately 35% of Firms used the services of an outsourced MLRO;

- over 80% of MLRO's held other positions within the Firm, the most common pairing being a Firm's Compliance Officer; and

- other pairings included being the Managing Director, Partner, Legal and Financial roles.

Whilst the DFSA does not prohibit dual roles, Firms should be mindful of potential conflicts of interests that may arise and individual resourcing limitations when appointing a MLRO.

The DFSA also notes the following concerns:

- Many Firms have centralised compliance and AML operations in another jurisdiction. While such arrangements may be advantageous in creating operational and commercial efficiencies, such arrangements should not usurp or replace the role of the MLRO. The MLRO as an individual authorised by the DFSA is accountable and responsible for ensuring such centralised functions are appropriate given the requirements of the AML Module; and

- A small minority of Authorised Firms (13%) had not appointed a Deputy MLRO[9] to fulfil the role of the MLRO in his/ her absence. Common justifications provided for this failure included that "the MLRO was always contactable" or that the Firm has decided against appointing a Deputy "on a risk-based approach". Such reasoning is not acceptable to the DFSA and fails to consider the adverse impact (however remote) of not having suitable coverage where the MLRO is absent.

Assessment of Business AML Risk (Section D1)

AML Rule 5.1.1 requires Firms to take appropriate steps to identify and assess money laundering risks to which its business is exposed, taking into consideration the nature, size and complexity of its activities.

Unless a Firm understands the money laundering risks to which it is exposed, it cannot take appropriate steps to prevent its business being used for the purposes of money laundering. Money laundering risks vary from Firm to Firm depending on the nature of its business, the customers it has, and the nature of the products and services being provided.

While the DFSA acknowledges that **Section D1** of the AML Return is the first time that Firms have been required to submit a copy of this assessment to the DFSA, the responses highlighted a need for significant improvement in this area.

---

[9] See AML Rule 11.2.3.

Examples of good and poor practices are included in the tables below:

Good Practices:

- the risk-assessment included input, discussion and acknowledgement from compliance, business lines heads and senior management and provided details as to how to mitigate each risk;
- individual consideration of relevant risk factors e.g. complex company or legal structures, risks posed by potential customers from particular jurisdictions, risks posed by specific products including trade finance and private wealth management;
- references to material and information supporting the analysis of AML risks e.g. FATF Mutual Evaluations reports, corruption indexes and AML indexes;
- an analysis of individual AML risks with conclusions on the likely impact these risks have on the business; and
- identification of risks requiring additional due diligence, but equally as useful identifying areas where the risks were lower and where simplified measures could be adopted.

Poor Practices:

- some Firms had not undertaken any assessment as required by AML Rule 5.1.1, leaving **Section D1** blank or referencing their AML policies and procedures which did not contain any assessment of AML risks;
- poor quality assessments of business AML risks included assessments which merely re-stated the requirements of the AML Module Rulebook without any tailored considerations of how these factors impacted the Firm. These assessments were vague and so high level that they could not have provided the Firm with any assistance in formulating their AML compliance programs; and
- some Firms provided generic risk managements reports which were not AML specific.

The conduct, quality and documentation of the assessment of business AML risks will remain a priority on the DFSA's AML supervisory agenda.

Assessment of Customer AML Risk (Section D4 & D5)

As required by AML Rule 6.1.1, a Firm must undertake a risk-based assessment of every customer and assign the customer a risk rating proportionate to the customer's money laundering risk. This includes:

- identification of the customer and any beneficial owners;
- ascertaining the purpose and nature of the proposed relationship;
- considering the customers country of origin, residence, nationality;
- considering the relevant product, service or transaction; and
- factoring in the outcomes of its business risk assessment.

The DFSA recognises that there can be overlap between the assessment of business and customer risks, though the assessment should nonetheless be carried out given that these assessments drive different elements of the AML compliance program. A business risk assessment is most informative and core to a Firm in developing its AML systems and controls, whereas a customer risk assessment is a key element in determining risk rating and ultimately determines the appropriate level of CDD.

Analysis of **Sections D4, D5 and E2** of the AML Returns indicated that overall, the majority of Firms are aware of the differing risk elements that should be considered in a customer risk assessment.

The majority of Firms were able to provide evidence of the consideration of the range of factors set out in AML Rule 6.1.1, through their policies and procedures, and provided templates and forms to document their analysis.

Examples of good and poor practices are included in the tables below:

Good Practices:

- a clearly documented formula and methodology for risk rating their customers, with differing and specific weightings placed on different risk elements such as product risk, quantum of customer investment, PEP status;
- development and implementation of above methodology into databases, spreadsheets and other electronic systems to enhance automation efficiencies and ensure consistent application and documentary evidence of the assessment;
- utilisation of the guidance provided by the DFSA (AML Rule Guidance 6.2.1 point 10) with respect to factors that may indicate a customer poses a higher risk of money laundering, or where such guidance is not applicable, the reasons for not considering the guidance is documented; and
- organised lists of their customers, categorising their AML risk and using such lists to inform their ongoing CDD e.g. risk reviews and screening.

Poor Practices:

- failure to document the reasoning behind the risk rating assigned to a customer;
- sole or over reliance on jurisdiction or country risk for determining a customer's risk rating. This approach fails to take into account that not all individuals from the same country will present the same overall AML risk;
- Firms taking a blanket approach to risk rating customers, either assigning all customers a standard risk or high risk regardless of individual risk elements.This was more prevalent in Firms with small customer numbers but can result in either not enough, or too much customer due diligence being undertaken. This is also likely to become problematic should customer numbers increase.

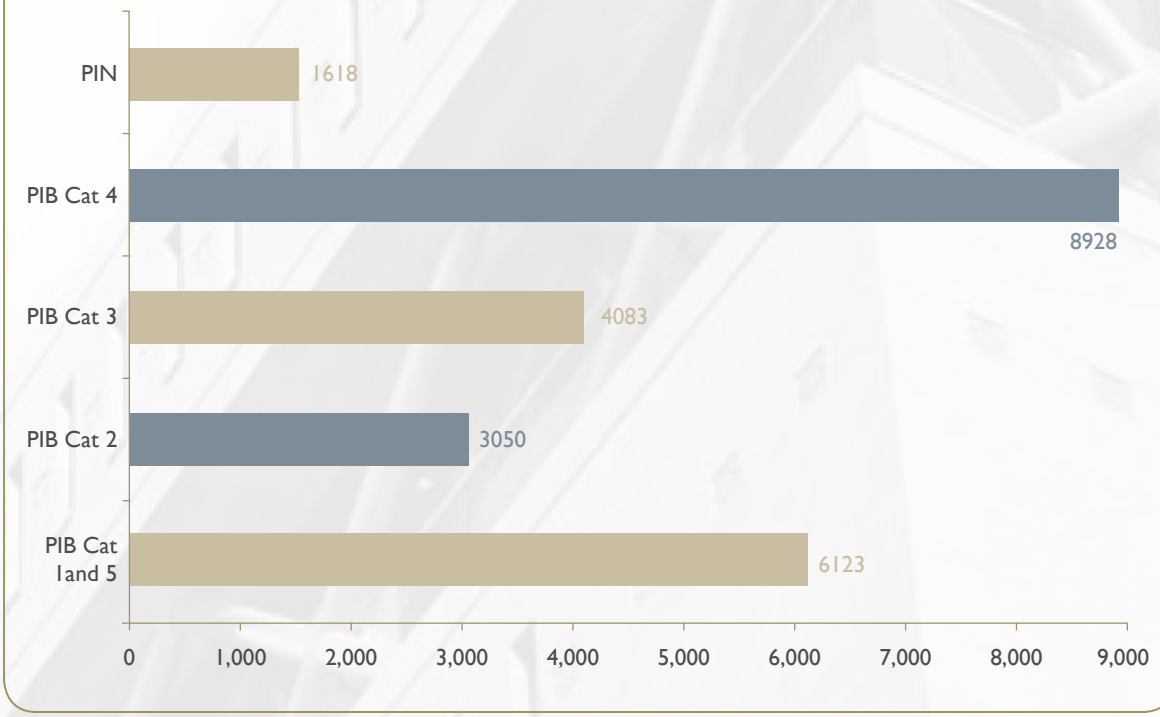
As indicated above, the analysis of customer AML risk as part of a Firm's overall risk-based approach will remain a priority of the DFSA's AML supervisory agenda.

Customers (Section E1)

The analysis of the AML Returns provides a good insight into customer numbers in the DIFC. The below tables indicate customer numbers broken down by prudential category, and further the customer risk rating assigned by the Firm of the sample reviewed.

Total Number of Customers by Firm Category

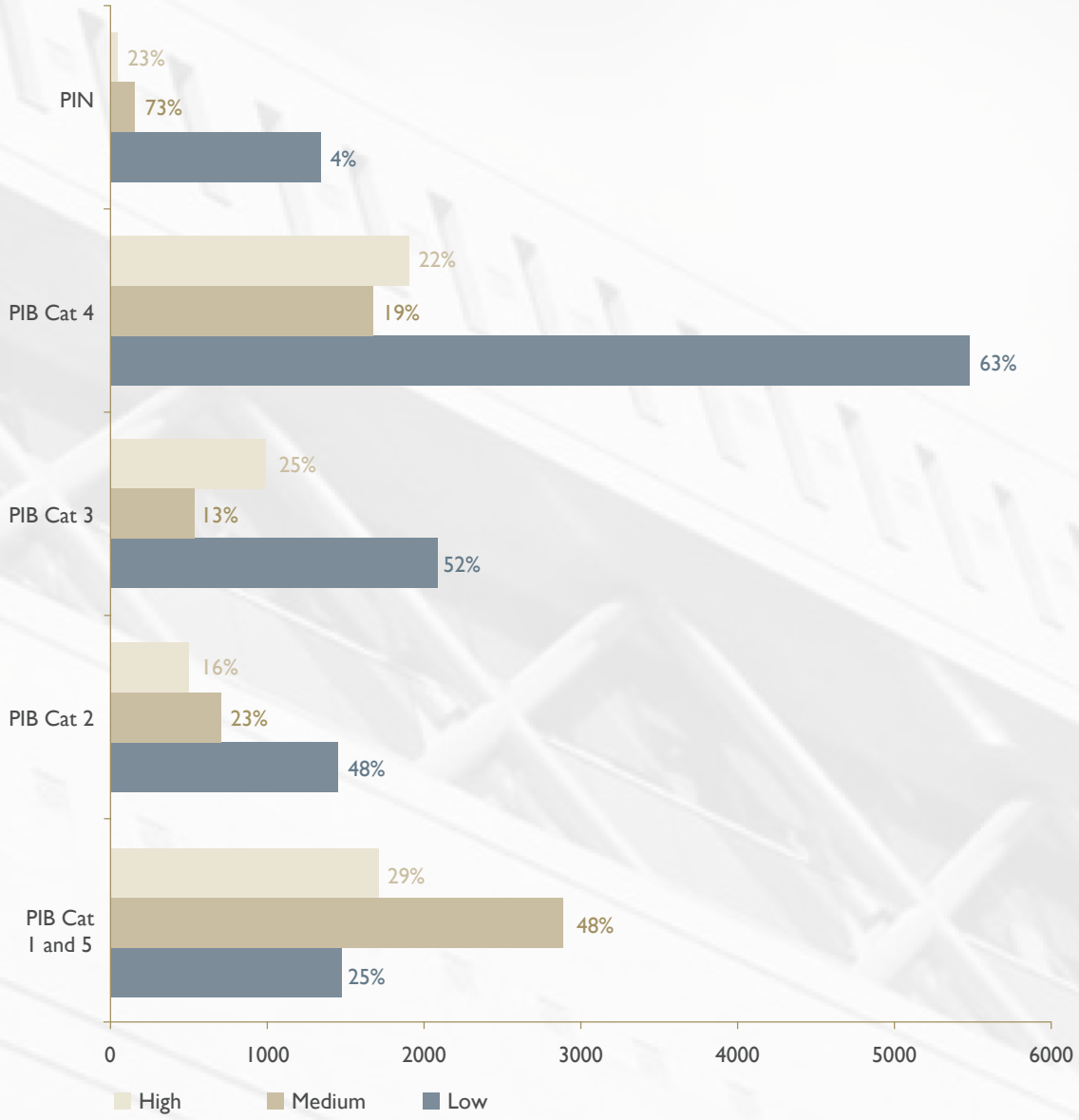
Total Number of Customers by Firm Category
Sample Size = 23,802 Clients



Breakdown of Customers by Risk rating per Firm Category

Total number of customers in sample size = 23,802 Clients

Sample size = 233 Authorised Firms



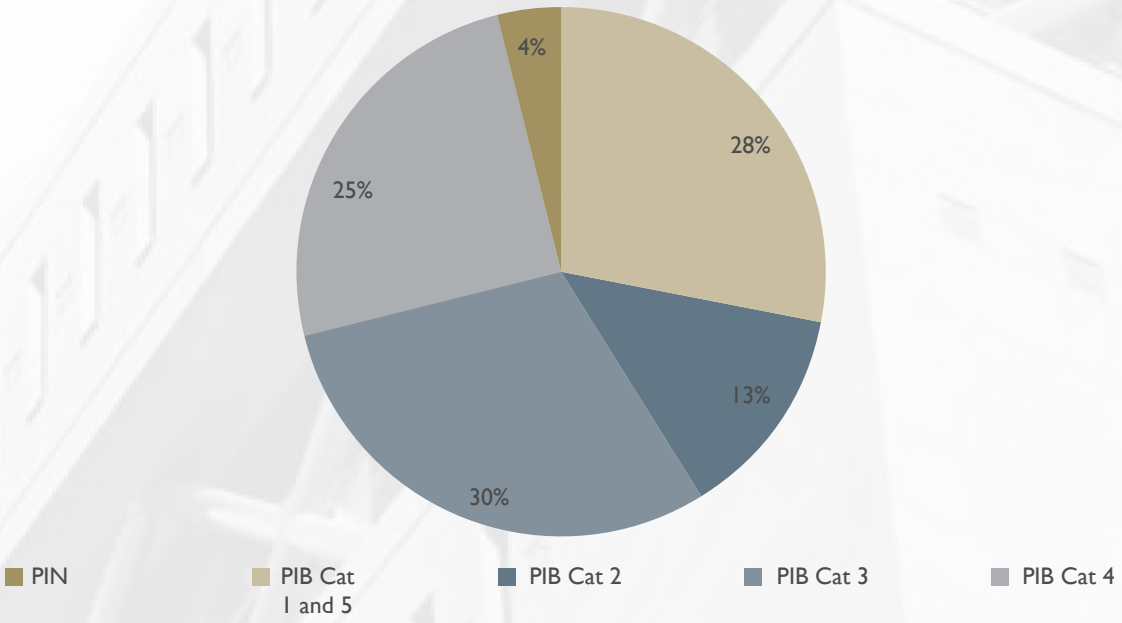
Politically Exposed Person (PEP) (Section E4)

In response to **Sections E4 and E5**, almost all Firms were able to provide an explanation of the systems used to determine whether a customer or beneficial owner was a PEP.These systems included third party screening and information vendors, internet searches and also PEP self declarations, with the best systems utilising all of these mechanisms.

Overall, 45% of respondents indicated that they had a PEP as a customer or had identified a PEP as a beneficial owner. The table below provides a breakdown of such respondents by prudential category of the sample reviewed.

PEPs per Firm Category

Total Number of PEPs = 2889 PEPs



Customer Due Diligence (CDD) (Section E6)

Firms should undertake CDD in a manner (risk-based approach) which is proportionate to the customer's money laundering risks.

The information in **Sections D2 and E6** of the AML Returns provided insight into each Firm's approach to CDD.

Examples of good and poor practices are included in the tables below:

Good Practices:
• CDD processes are well documented and in plain English; • inclusion of flow charts and other aids to describe how CDD should differ for different AML risks; and • stressing that business cannot commence with a customer unless CDD is completed.

Poor Practices:
• the lack of any meaningful differentiation between the levels of CDD. In an extreme example, the only difference in enhanced due diligence measures was obtaining one extra form of identification; and • some Firms took a blanket approach to CDD, electing to apply the same level of CDD to all its customers. Such an approach is seen as being cautious if a higher level of CDD is applied than would be required, but it can also result in less CDD being completed in higher risk circumstances.

While not specifically considered in the report, the DFSA will continue to focus on how a Firm documents its understanding and verification of source of funds and source of wealth.

Ongoing CDD (Section E7 & E8)

AML Rules 7.6.1 and 7.6.2 set out the DFSA's requirements relating to conducting ongoing CDD which includes:

- monitoring transactions undertaken during the course of its customer relationship to ensure that the transactions are consistent with the Firms knowledge of the customer;
- paying particular attention to any complex or unusually large transactions or unusual patterns of transactions that have no apparent or visible economic or legitimate purpose; and inquire into the background and purpose of these transactions ;
- reviewing periodically the adequacy of the CDD information it holds on customers and beneficial owners to ensure that the information is kept up-to-date;
- reviewing periodically each customer to ensure that the risk rating assigned to a customer remains appropriate for the customer; and
- reviewing its customers, their business and transactions against United Nations Security Council sanctions lists and against any other relevant sanctions lists (e.g OFAC, EU & HMT).

An unexpectedly high number of Firms answered "not applicable' or provided no answer to **Section E7,** which sought an explanation of how a Firm undertakes ongoing monitoring of its customers and their transactions.

Transaction Monitoring

It was observed from the AML Returns that many respondents erroneously relied on the fact that transactions were booked in locations outside the DIFC to not answer this question.

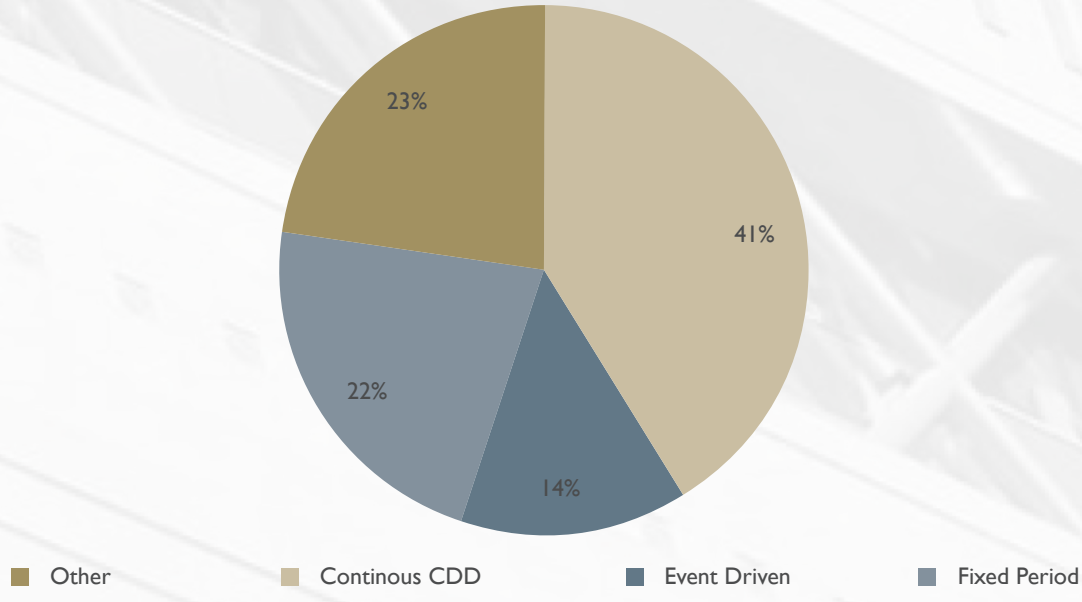
- In such circumstances, the DFSA accepts that while any AML risk is shared with the booking location, this does not remove the responsibility from the DIFC Firm to monitor transactions to ensure that they are consistent with their knowledge of the customer;
- a Firm's transaction monitoring program should take such circumstances into consideration, and where monitoring is undertaken at the booking centre, the DIFC Firm should ensure that the findings and alerts generated from this system are shared. This may include the lodgement of SAR in both jurisdictions; and
- where appropriate a Firm may place reliance on a third party entity, but such reliance should adhere to the DFSA's requirements in Chapter 8 of the AML Module. A Firm may also consider whether additional comfort can be gained from periodic sample testing of "relied upon' processes.

Review of CDD Information

Section E8 of the AML Return concerned the frequency of a Firm's review of the adequacy of CDD information it held on its customers and beneficial owners. An analysis of this information (which is summarised in the chart below) revealed that:

- 41% of respondents conducted continuous or rolling reviews of their CDD, which allowed the workload to be spread over time;
- 22% of respondents had a fixed date in which CDD for all customers was reviewed;
- 14% of respondents used an event driven process for review, triggered only when new information was brought to light about the customer or when a new service or transaction is requested; and
- 23% of respondents used a variety of other means, including monitoring being driven from a parent or other group entity; or were newly authorised Firms with no or very small customer numbers.

Ongoing CDD Review Frequency



Examples of good and poor practices are included in the tables below:

Good Practices:
• the ongoing CDD process is clearly described in AML policies, these were supplemented by compliance calendars which set out the key review dates; • Firms using software solutions and platforms to automatically screen against sanctions lists and customer transactions; • CDD information is electronically captured with accompanying flags which indicated expiry of static information such as passports and IDs; and • screening software scrubs against batch lists of key names and entities including customers, beneficial owners and known associates, on an ongoing basis, generating real time alerts.

Poor Practices:
• reviews which were initiated only when a customer informed of changes, for example change in address; or where the RM became aware of changes through ad hoc means as opposed to designated review dates; • reviews only being initiated when a new service or product is requested which do not take account of non transaction risk factors, such as listing on a sanctions list, or change in customer details; • over reliance on screening software, without sufficient evidence of operational understanding of how software works. Firms should understand how screening software operates and which data is being searched; • sole reliance on third parties without meeting DFSA requirements, or in circumstances where the Firm does not understand the nature of the monitoring being undertaken by the third party; and • CDD information only gathered and analysed at on-boarding stage but then not subject to any review.

Firms' ongoing CDD policies, procedures, systems and controls are one of the most important aspects of effective CDD. Given the DFSA observations regarding deficiencies (poor practices) in implementing ongoing CDD, this area may also be explored further through a number of supervisor tools including thematic reviews.

Reliance and Outsourcing (Section F1 & F2)

Sections **F1 and F2** of the AML Return relates to placing reliance on and/or outsourcing elements of CDD to third parties. Chapter 8 of the AML Module was designed to allow Firms to place reliance on specified third parties to conduct one or more elements of CDD on its behalf. The specified third parties include:

- another Authorised Firm;
- a law firm, notary or other independent legal business, accounting firm, audit firm or insolvency practitioner or an equivalent person in another jurisdiction;
- a financial institution; or
- a member of the firm's group.

Notwithstanding a Firm placing reliance on or outsourcing to a third party, the Firm remains responsible for compliance with, and liable for any failure to meet the CDD requirements of the AML Module.

In order to avail itself of the benefits of this provision, a Firm must satisfy the requirements set out in AML Rule 8.1.1(3).

Based on the sample reviewed, over 33% of respondents stated that they placed reliance on, or outsourced one or more elements of their CDD. However, the DFSA is concerned that this statistic is unreliable because a significant portion of respondents may not have understood this question, or, did not have an understanding of the parameters of Chapter 8 of the AML Module.

Some general responses which may have unintentionally skewed the analysis of this information included:

- Firms interpreting the use of a third party information vendor or screening software as a mode of reliance. Such services are not captured within the scope of Chapter 8, as the Firm is analysing the resultant search information and drawing its own conclusions. In other words, while information may be being provided by a vendor, it is the Firm who is still considering and processing it to determine what, if any impact it should have on their respective risk assessments; and
- Firms using outsourced MLROs also may have incorrectly included such activity within the ambit of the Reliance section and merely replicated their answers within the Outsourcing section of the AML Return.

The answers provided in this section of the AML Return highlight the importance of respondents reading the question carefully and applying answers within the context of the Rule reference provided.

Audit (Section G1-3)

AML Rule 9.4.1 requires an AF to ensure that its audit function includes regular reviews and assessments of the effectiveness of the its money laundering policies, procedures, systems and controls, and its compliance with the obligations of the DFSA AML Module.

These reviews may be undertaken internally by the Firms internal audit function, or externally by a competent Firm of independent auditors or compliance professionals.

74% of respondents confirmed that they had conducted an audit on their AML policies, procedures, systems and controls, though the findings of these audits were not always provided as required by **Section G2**.

In respect of those respondents who did not conduct such an audit, common reasons for the failure to do so included:

- the Firm was recently licensed or had a change in status;
- the internal audit was ongoing during the reporting period; or
- the Firm had no clients and therefore could not conduct any meaningful reviews.

There was a small minority of Firms who indicated that they did not have an internal audit function, or that AML was not included in the scope of their audits. The DFSA would expect that such internal mechanism are in place and include an AML component which is routinely reviewed. Without valid or reasonable excuse such Firms are in breach of both the AML and GEN Module.

Sanctions (Section H1-2)

The DFSA expects Firms to establish and maintain effective systems and controls to obtain and make appropriate use of relevant resolutions, sanctions, findings, recommendations, guidance, directives, notices or other conclusions issued by:

- the United Nations Security Council;
- the government of UAE or any government departments in the UAE;
- the Central Bank of the UAE or the AMLSCU;
- FATF;
- UAE enforcement agencies; and
- the DFSA.

The DFSA also expects Firms to take its own steps in acquiring relevant information from various available sources such as obtaining relevant information from consolidated list of financial sanctions in the European Union Office, HM Treasury (United Kingdom) lists, and the Office of Foreign Asset Control (OFAC) of the United States Department of Treasury.

The following practices were observed from our analysis of the AML Returns:

- 96% of respondents confirmed that they had systems and controls in place to make use of relevant sanctions and other international obligations referred to in Chapter 10 of the AML Module;

- 4% did not have such systems and controls provided explanations, for example, that their only customers were group entities, or that such monitoring was done at by a parent entity. For abundant clarity, these Firms should nonetheless have systems in place to comply with this rule, though they can be simplified given the lower sanctions exposure, or be subject to the reliance provisions in the AML Module (Chapter 8);

- the most predominant support tool of these systems and controls was the use of third party information vendors and database providers. Such providers allow for relevant customers to be screened using software which is continuously updated with sanctions listings;

- 85% of respondents indicated they used sanction screening software;

- 15% relied upon systems that involved manual checking of a customer against relevant sanctions lists. Such an approach may be appropriate where a Firm's customer numbers are low and manageable, but are vulnerable to human error and can be time consuming;

- in relation to the frequency of sanctions screening and checks, 54% of respondents indicated that they conducted real time or continuous screening of their customer details using their software solutions; and

- 34% of respondents conducted regular fixed period screening, be it quarterly or as part of scheduled CDD refreshes.

AML Training and Awareness (Section 11-4)

The DFSA expects Firms to provide AML training to all relevant employees at appropriate and regular intervals. The AML training should be appropriately tailored to the Firms' activities, including its products, services, customers, business partners, level and complexity of its business and transactions.

In the case of AFs, the DFSA expects that training should be provided to each relevant employee at least annually.

The AML Returns indicated that 82% of Firms provide AML training on an annual basis, with the balance using a variety of other methods such as on induction for new starters, quarterly updates or on an ad hoc or issues driven basis e.g. recent regulatory actions or outreach.

The most popular mechanism for providing AML training was "in-house presentations" conducted in a group environment, but other forms of training included web based platforms, external courses and other self-learning initiatives.

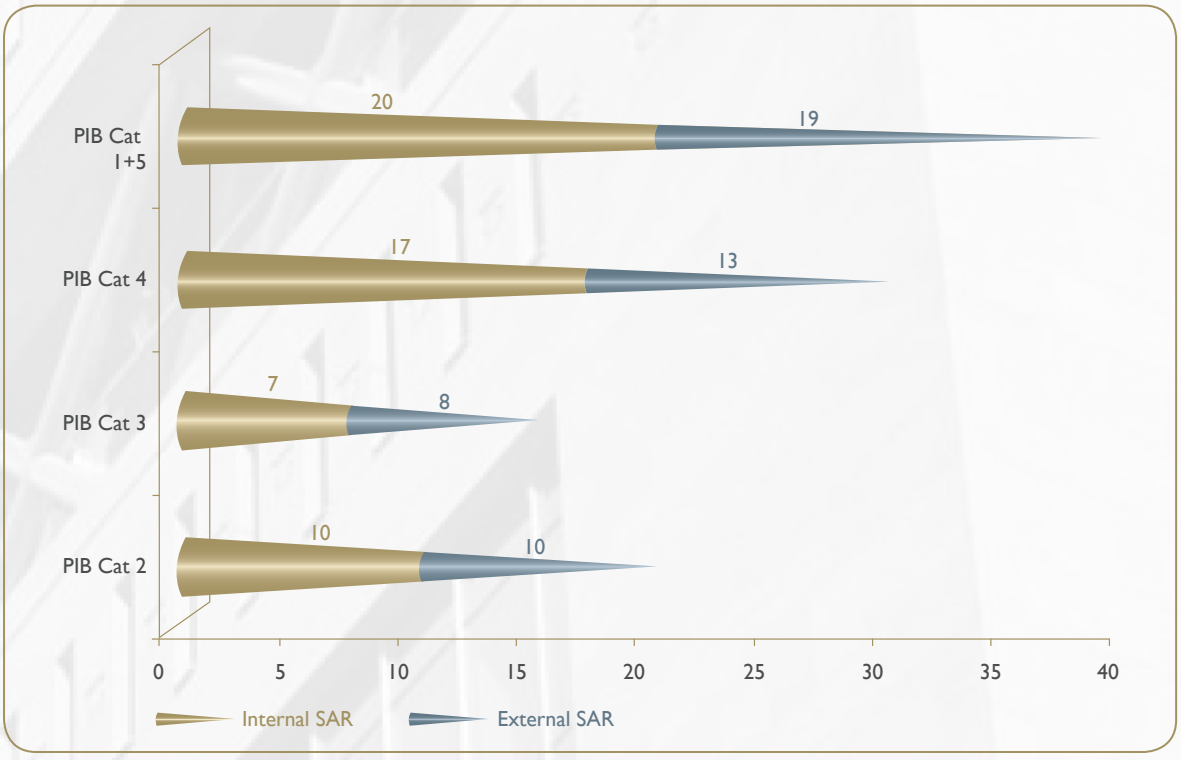
Irrespective of the way in which training is delivered, it is important for Firms to maintain training log records so that they can ensure that employees are appropriately trained and have their knowledge refreshed at appropriate intervals.

Suspicious Activity Report (SAR) (Section J1-3)

The obligation to lodge SARs with the AMLSCU is created in the UAE Federal Law regarding AML (No 4 of 2002, amended by Federal Law No 9 of 2014) and mirrored in Chapter 13 of the AML Module. The following includes (but not limited to) the DFSA's expectation as to appropriate practices:

- the making of such reports should not be considered merely a reporting requirement for MLROs, but the conclusion of a process of escalation and investigation of suspicious activities and transactions;
- often overlooked by Firms is the requirement for policies and procedures, systems and controls to include mechanisms in which employees are able to communicate suspicions to the MLRO;
- such notifications should be encouraged and employees should be erring on the side of caution when making such notifications to ensure that activities and transactions, even if minimally suspicious, are escalated for consideration; and
- once an employee notification is made, it is then the MLRO's obligation to investigate and document the circumstances under which the notification was made, and determine whether an SAR to the AMLSCU is required. Not all internal notifications should result in an SAR, though all notifications should be investigated and the reasoning behind the decision documented.

Based on sample review, a total of 54 internal notifications were made by the respondents, which resulted in 50 SARs being lodged with the AMLSCU. A breakdown by Firm submission is included below:



The number of internal notifications made by respondents is of interest, as the DFSA expects that the basis or trigger for submitting an internal notification should be as expansive as possible, with the MLRO then acting as a second stage filter and ultimately deciding if an SAR is required. The DFSA therefore expected that the number of internal notifications would be significantly higher than the number of external SAR reported.

The DFSA encourages all Firms to promote and re-iterate the importance of internal notifications by employees. In particular, that the threshold of suspicion should be considered low and a conservative approach taken. MLRO's should then utilise their expertise to investigate and make a decision as to whether that suspicion warrants an SAR.

The close correlation of the number of internal notifications to external SARs could indicate that:

- internal notification systems are being too tightly calibrated resulting in minimal notifications; or
- internal notifications may not be being properly documented or recorded.

The number of external SARs reported to the AMLSCU continues to trend upwards year on year, the reported AML Return results support this trend continuing. The DFSA would expect this volume to continue to increase as Firms become more efficient and familiar with the requirement to lodge SARs.

The DFSA hopes to gain a more detailed understanding of a Firm's internal notifications and external SAR reporting processes and will continue to test these as part of its AML supervisory agenda.

Preparing your next Annual AML Return

Following the DFSA's review and analysis of the first set of AML Returns, the DFSA provides the following guidance for the preparation of Firms' AML Returns.

Finding the AML Return and its Due Date

- The Annual AML Return is located in the DFSA's AFN Module published on the DFSA website. Your Firm should ensure that the latest version is used and submitted.

- Your Annual AML Return is due within four months of your financial year end. Thus, if your financial year end is 31 December, you are required to submit your AML Return by 30 April.

Your Firm should ensure that they allow themselves sufficient time to involve senior management in the completion of this return. Should you require additional time to submit the AML Return, any requests for an extension should be made to the DFSA in advance of the due date. A failure to submit on time is a Rule breach.

Guidance on submitting your Annual AML Return

1. Consider the observations and findings contained in this report with specific attention to the deficiencies highlighted by the DFSA analysis.

2. Read each question carefully and ensure that all questions are answered including sub-questions.

3. Refer to the Rule references which are attached to each section before answering, as not all sections may be applicable. These references will provide context and guidance to the anticipated response.

4. Attach all supporting documentation relevant to the question being asked and provide specific references (page and paragraphs) to these documents where required.

5. You are not required to attach supporting documentation where it has been provided to the DFSA in your previous AML Return, unless such documents have been updated or amended. Your answers should reference that you have previously provided such documents and that they have not changed.

6. If a date is requested provide an actual date or explain why no date is available.

7. Where you are unable to provide an answer, or a question is "not applicable", you must explain why you are unable to provide the answer or why the question is not applicable.

8. Do take into account any specific comments provided by the DFSA on your previous AML Return submission.

Tel: +971 4 362 1500
Fax: +971 4 362 0801
PO Box 75850
Level 13, The Gate, Dubai, UAE
Website: www.dfsa.ae