By Email

23 February 2024

To Senior Executive Officers, Compliance Officers and Money Laundering Reporting Officers of DFSA Authorised Firms

Key Themes and Findings from 2023 DFSA Risk Assessments: Private Banking Business Models

In line with our regulatory objectives, and our 2023 supervisory priorities, the DFSA conducted a series of on-site risk assessments of Authorised Firms ('firms') operating private banking business models. The focus of the risk assessments was to assess firms' compliance with regulatory obligations relating to the General (GEN), Conduct of Business (COB), and Anti-Money Laundering, Counter-Terrorist Financing and Sanctions (AML) Modules of the DFSA Rulebook.

The purpose of this letter is to share the key themes and findings arising from our risk assessments to promote best practice, high standards of regulatory compliance, and wider improvements across the industry.

Background

The DFSA adopts a risk-based approach to supervising firms, focusing our resources on those firms that pose the highest risks to our regulatory objectives. This is shaped by the nature, scale and complexity of each individual firm and the risks it poses. On-site risk assessments are one of the key supervisory tools we use to assess the adequacy of firms' systems and controls, and identify risks to DFSA objectives.

Private banking and wealth management remains a key sector in the DIFC and enhances its position as a global financial hub. The significant interest and growth in this sector are also reflected in relevant firms reporting circa $84bn of assets under advisory for over 12,000 clients, an increase of circa 23% from 2022 year end reporting. We continue to receive new licensing applications from applicant firms seeking to operate this business model in or from the DIFC, however, this model presents certain risks which require mitigation by firms, including inherently higher risk exposures to financial crime.

This letter summarises the key themes and findings from our 2023 cycle of risk assessments, which represented over 90% of the assets under advisory in this sector. These risk assessments involved on-site visits to interview senior management, including Senior Executive Officers, Compliance Officers, Money Laundering Reporting Officers, and other relevant staff, together with desk-based reviews of policies and procedures, management information, and training materials.

Key findings

Below is a summary of the key themes and findings relating to firms' compliance with the GEN, COB, and AML Modules of the DFSA's Rulebook. The findings are detailed further in the Annexes to this letter.

Weaknesses were identified in the following areas:

General and Conduct of Business Compliance
- Firms' governance arrangements
- Resourcing of the compliance function
- Compliance with the client suitability requirements
- Client classification processes and procedures
- Outsourcing and reliance on Head Office/other Group entities
- Handling of staff related misconduct

Financial Crime Systems and Controls
- Assessing business AML risks
- Assessing customer AML risks
- AML systems and controls
- Enhanced Customer Due Diligence
- Ongoing Customer Due Diligence
- Suspicious Activity Reports
- Outsourcing
- AML Training and Awareness

Next steps

We will elaborate on the key themes and findings from our risk assessments in an upcoming outreach session specifically for private banking business models.

The DFSA expects all firms operating private banking business models in or from the DIFC to consider these key themes and findings in the context of their specific activities and obligations. While the risk assessments were focused on a specific business model, some of the findings likely apply more widely across firms. The DFSA expects all firms to take note of this letter and consider further enhancements to their systems and controls (where appropriate). In future engagements with the DFSA, firms will be requested to demonstrate how they did so.

We also remind firms of their continuing obligations to ensure that the DFSA is promptly informed of any significant events or anything else relating to the firm of which we would reasonably expect to be notified.

If you have any questions in relation to this letter, or more generally, please contact us via the Supervised Firm Contact Form found on the DFSA's website.

Yours sincerely,

Mohamad El Khalil
Managing Director (Acting), Supervision

Annex A: Key Themes and Findings from Risk Assessments of Private Banking Business Models – General (GEN) and Conduct of Business (COB) Modules of the DFSA Rulebook

Finding 1: Firms' governance arrangements (GEN 4.2.11/5.2/5.3.2/5.3.3)

We expect firms to have a corporate governance framework in place that is appropriate to the nature, scale and complexity of their business and structure, which is adequate to promote the sound and prudent management and oversight of its business and to protect the interests of its customers and stakeholders.

We observed weaknesses in firms' governance arrangements, including a lack of clarity on the roles, responsibilities, and reporting lines of senior management. Specific examples included:

- Senior Executive Officer not having the required level of ultimate responsibility and accountability for key business lines and functions of the firm; and
- Overlap in responsibilities between key individuals and functions of the firm.

In addition, where senior management are subject to dual reporting lines both at the firm and Group level, firms should ensure this does not lead to confusion in terms of accountability and decision making. Firms must ensure that proper segregation of duties and independence of key functions is maintained.

Action: Firms must review the adequacy of their current governance arrangements (including but not limited to roles, responsibilities, and reporting lines of senior management) to ensure they are appropriate and aligned to the nature, scale, and complexity of their business activities.

Finding 2: Resourcing of compliance function (GEN 5.3.7/5.3.9)

Firms must establish and maintain compliance arrangements, including processes and procedures that ensure and evidence compliance with all legislation applicable in the DIFC. Firms must also ensure that the Compliance Officer has access to sufficient resources, including an adequate number of competent staff, to perform their duties objectively and independently of operational and business functions. Failure to meet these requirements could result in regulatory breaches not being identified and/or existing systems and controls not operating effectively.

In several risk assessments, we identified inadequacies in the resourcing levels and capacity of the compliance function.

Action: Firms must review the adequacy of their current compliance resources to ensure that their systems and controls are appropriate to the nature and extent of the firm's business, including the pace of business growth. Where appropriate, firms should strengthen their compliance functions by increasing staff resources.

Finding 3: Compliance with the suitability requirements (COB 3.4)

The DFSA has highlighted suitability as a priority area, and also published the DFSA's Thematic Review on Suitability[1] in 2021. Despite this, we continue to observe firms failing to demonstrate compliance with DFSA Rules on suitability.

Compliance failings concerning suitability were a recurring issue across our cycle of 2023 risk assessments. Overall, we observed that firms need to take further actions and measures to improve their suitability frameworks and related record-keeping practices.

In several instances, we observed that suitability assessments were generic and lacking in detail, with certain firms adopting a tick-box approach. In particular, we observed a lack of documented rationale as to why a particular product had been recommended over another.

Action: Firms must review the adequacy of their suitability frameworks to ensure they are aligned with applicable DFSA Rule requirements, notably COB 3.4. Any deficiencies must be addressed as a priority.

Finding 4: Client classification processes and procedures (COB 2)

Then DFSA observed continuing deficiencies in firms' approaches to client classification despite our previous 2017[2] thematic review on this area and subsequent follow up work. Firms must demonstrate they are fully compliant with DFSA Rules on client classification This is a supervisory priority for the DFSA.

Identified deficiencies included unsatisfactory assessments of clients' knowledge and experience, lack of supporting rationale and verifiable information to evidence the assessment. Certain firms are applying a tick-box approach. Furthermore, we observed limited challenge from firm's compliance functions and/or a lack of compliance monitoring of the effectiveness of the firm's client classification framework.

Action: Firms must review the adequacy of their client classification processes and procedures to ensure they are aligned with applicable DFSA Rule requirements, notably COB Chapter 2. The compliance function must exercise its responsibilities appropriately in that respect. Any deficiencies must be addressed as a priority.

Finding 5: Outsourcing and reliance on Head Office/other Group entities (GEN 5.3.21)

In our experience, private banking business models in the DIFC (usually branches or subsidiaries of foreign entities) typically involve close collaboration with and reliance on the policies, procedures, and resources of Group entities. In certain instances, we observed failures to give proper consideration to DIFC and DFSA requirements in firms' policies and procedures. We also observed instances of certain firms' functions being performed by Group entities resulting in the individual with responsibility and oversight for the particular function in the DIFC being unable to demonstrate sufficient understanding of that function (and/or its operations and performance).

[1] Thematic Review on Suitability 2021
[2] DFSA's Client Classification and Suitability Thematic Review 2017

We remind firms of their obligations under GEN 5.3.21, where a firm outsources functions or activities to service providers (including within its Group), it is (i) not relieved of its regulatory obligations; and (ii) remains responsible for compliance with legislation applicable in the DIFC.

Action: Firms must review their oversight arrangements of any key functions or activities outsourced to Head Office/Group entities, and related processes and procedures, to ensure they are adequate to meet applicable DFSA Rule requirements.

Finding 6: Handling of staff related misconduct (GEN 5.3.18/19)

We remind firms of their obligations to ensure their employees remain fit and proper. This includes implementing appropriate systems and controls and maintaining required relevant records.

During our 2023 risk assessments and engagement with firms, we observed instances of:

- Firms failing to carry out sufficient background checks or due diligence during their recruitment process to identify whether applicants have a record of previous misconduct or issues that could impact their employment with the firm; and
- Delays in taking appropriate action concerning employee misconduct, or, in some cases, firms failing to take any appropriate disciplinary action.

We also observed certain instances where firms were deficient in implementing staff training, including in relation to the firm's regulatory obligations in the General and Conduct of Business Modules of the DFSA Rulebook. Failure to ensure staff are adequately trained may increase the risk of regulatory breaches and/or conduct risks materialising.

Action: Firms must review the adequacy of their systems and controls relating to staff and agents, including HR disciplinary processes and training programs, to ensure their staff are appropriately trained and any instances of serious misconduct are identified and addressed appropriately in a timely manner.

Annex B: Key Themes and Findings from Risk Assessments of Private Banking Business Models – Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Module (AML) of the DFSA Rulebook

Finding 1: Assessing business AML risks (AML 5.1)

The DFSA identified various deficiencies in the quality of the Business AML risk assessment (BARA), including:

- certain firms did not have a clear business risk assessment and scoring methodology
- BARAs excluded either inherent risk, controls effectiveness, or residual risk ratings
- BARAs were too generic and not sufficiently detailed to allow the user to understand the risks
- no quantitative data being considered to support the conclusions reached in an objective manner
- BARAs omitted certain inherent risk factors set out in the AML Module e.g., risks arising from the use of new or developing technologies and the development of new products and business practices, including new delivery channels and partners
- BARAs omitted a detailed assessment of Targeted Financial Sanctions (including proliferation financing)
- BARAs failed to evidence that the outcomes of the UAE National Risk Assessment (NRA) were considered in the assessment (as relevant to the firm's business model)

Inadequate BARA processes may result in firms failing to identify and assess AML risks to which their businesses are exposed resulting in failures to implement appropriate AML systems and controls.

Action: Firms are reminded of their obligations to identify and assess money laundering, terrorist financing and proliferation financing risks, to which their business is exposed, taking into consideration the nature, size and complexity of their activities, as mandated in Chapter 5 of the AML Module.

Finding 2: Assessing customer AML risks (AML 6.1)

The DFSA identified various firms having inadequate or unclear customer risk assessment (CRA) risk scoring methodology. In certain instances, the CRA methodology omitted certain risk factors e.g., nature of business, product/services risk, and other source of wealth jurisdictions, where a client's wealth was generated from multiple jurisdictions. We also identified instances where the customer's risk rating was amended during ongoing review with no clearly documented reasons.

Inadequate CRA processes may result in firms failing to identify the correct level of risk posed by both new and existing clients, and the appropriate extent of due diligence measures to mitigate those risks.

Action: Firms must establish an adequate customer risk assessment framework to meet applicable DFSA Rule requirements, including as set out in AML 6.1.1.

Finding 3: AML systems and controls (AML 5.2)

The DFSA observed that certain firms' AML policies and procedures were inadequate due to not being customised to the firm's business activities and processes. Certain of these policies and procedures simply duplicated the AML Module and lacked detailed operational procedures and guidance for employees.

Certain firms simply relied upon their Group sanctions procedures and lacked detailed local operational procedures necessary to comply with the UAE Targeted Financial Sanctions requirements. For example: roles and responsibilities, screening standards, turnaround times, funds freezing procedures, funds freezing reporting, and partial name match reporting.

We also observed instances where firms lacked sufficient detail in their management information / metrics covering key AML processes e.g., CDD file reviews, transaction monitoring alerts, screening alerts, suspicious transaction reporting, and quality assurance results. These information deficiencies hamper effective local senior management oversight and consideration of key risks in local governance committees.

Action: Firms must ensure they establish and maintain effective AML policies, procedures, systems, and controls, which are tailored to the nature, scale, and complexity of their business activities.

Finding 4: Enhanced Customer Due Diligence (AML 7.4)

The DFSA observed most firms as having reasonably adequate Enhanced Due Diligence (EDD) procedures in place. However, DFSA client file reviews revealed deficiencies in corroboration of source of funds (SOF) and source of wealth (SOW) for high-risk clients, including limited SOW journey narratives, lack of supporting evidence or documents, and/or over-reliance on benchmarking, or inappropriate application of benchmarking.

Action: Firms must implement robust EDD procedures, including appropriate corroboration steps, to ensure compliance by relevant employees responsible for conducting customer due diligence and approving high risk client files.

Finding 5: Ongoing Customer Due Diligence (AML 7.6)

The DFSA observed instances where certain firms failed to conduct periodic reviews in accordance with their established cycle for standard risk clients, with backlogs greater than 6 months past due date.

In certain instances, the DFSA observed that ongoing due diligence measures were not properly applied, leading to incomplete and outdated KYC documents in the client file, and review comments were sporadic and did not include commentary on the review of the client's transactional activity patterns. In such instances, no meaningful challenge was provided by the checker / approver from the operations function or the compliance / AML team, thereby rendering the control mechanism ineffective.

Ineffective ongoing CDD may inhibit a firm's ability to identify, assess, and mitigate, potential money laundering risks on an ongoing basis.

Action: Firms must implement effective procedures, systems and controls, and monitoring mechanisms, to ensure ongoing customer due diligence is conducted effectively and in a timely manner in accordance with applicable DFSA Rules.

Finding 6: Suspicious Activity Reports (AML 13.2/13.3)

The DFSA's review of 2023 AML Returns revealed a 74% increase in the number of internal notifications reported to the MLRO from the previous 2022 AML Return. Similarly, the DFSA observed a 35% increase in the number of suspicious activity reports (SARs) from the private banking sector.

The DFSA also observed instances where filed SARs lacked detailed context and key information such as account balances, assets under management, source of wealth, and other connected accounts. Weak SARs reporting procedures may result in a breach of both Federal AML legislation and DFSA administered legislation.

Action: Relevant Persons must establish and maintain policies, procedures, systems and controls, to monitor and detect suspicious activity or transactions in relation to potential money laundering or terrorist financing and report to the FIU.

Finding 7: Outsourcing (AML 8.2)

As mentioned in this letter, many firms operating a private banking business model in or from the DIFC are branches or subsidiaries of financial institutions. The DFSA observed that certain firms did not have clearly defined service level agreements (SLAs) with relevant Group entities setting out roles and responsibilities, quality standards and reporting for internally outsourced AML processes (i.e., transaction monitoring, name, transaction screening, and ongoing CDD). As a result, there was no evidence of MLRO and local senior management oversight and assurance of these outsourced processes.

AML 8.2.1 provides that a Relevant Person which outsources any one or more elements of its customer due diligence to a service provider (including within its Group) remains responsible for compliance with, and liable for any failure to meet, such obligations.

Action: Firms must ensure there is a clearly documented binding agreement, including service standards, with any outsourced service providers.

Finding 8: AML training and awareness (AML 12.1)

The DFSA observed that certain firms had not arranged proper staff training on targeted financial sanctions risks as part of the firm's overall staff training program. Certain firms' training materials were only high level and failed to cover key aspects such as applicable UAE legislation, circulars and guidance issued by the Executive Office for Control and Non-Proliferation; roles and responsibilities; implemented screening systems and controls; red flags; evasion techniques; case studies or examples applicable to the business model; and funds freezing and related reporting mechanisms.

The DFSA also observed that certain AML training was generic and the same for all employees. There was no specialised and tailored training for front line and support staff involved in client onboarding and ongoing customer due diligence processes.

Action: Firms must implement comprehensive AML training and awareness program for their staff which is appropriately tailored to the firm's activities including its customers, distribution channels, business partners, and complexity of its products, services, and transactions.