

THE **AMLATF** BOARD

MITIGANTS QUESTIONNAIRE

I - GENERAL INFORMATION

1. Name of RPF: _____

2. Reporting date: _____

3. Names and surname of the Managing Partner or Equivalent:

4. Names and surname of the MLRO/Compliance Officer:

Guidelines for the completion of:

AML/CFT CONTROLS QUESTIONNAIRE

1. The Questionnaire is designed to gather information on a periodic basis to assist in assessing the quality of internal control systems in place for AML/CFT purposes. It is one of a number of inputs into an overall AML/CFT risk-profiling system.
2. RPFs should complete the following first 3 columns:

Risk Mitigants (risk management, controls, compliance, etc.)	Yes/No	RPF's Description/Comments MANDATORY
---	--------	---

Column 1 provides scope for the RPF to describe the AML/CFT mitigants (policies, controls, procedures, etc.) they have in place (or, where appropriate, plan to introduce or improve them.

Column 2 is a Yes or No answer depending on whether or not there any mitigants in place. In the case of a Yes response, then Column 3 should be completed.

Column 3 should contain a concise description of the mitigant, which would also describe the RPF's compliance with the applicable AML Law, Regulations and/or Guidelines.

3. Suggestions are made [*in italics within square brackets*] for documents to accompany the completed questionnaires. It is for the authorities to decide in each instance whether these documents are necessary or useful. If not, these suggestions may be deleted.
4. In completing the Questionnaire, RPFs should not leave any questions unanswered. For any questions that are not relevant to the business of the particular RPF, insert 'N/A' with an explanation as to why it is not applicable.
5. Each of the 5 mitigants Sections begins with a statement of Requirement/Control. Where possible, the text in each case should be replaced by the Board/Managing Partners with the appropriate obligation quoted from the AML Law, regulation, etc., to tailor the Questionnaire as much as possible to the Bermudian requirements. The legal/regulatory/guidance citation is to be included by the Board/Managing Partners in column 4.
6. The last column is reserved for an assessment for the Board/Managing Partners supervisor – based on his/her knowledge of the RPF, including that gained from previous on-site inspections. In addition to indicating whether or not the RPF's response is plausible and reliable, it is suggested that the last column be used to indicate the need for any further steps – additional information requirements or follow-up action – which could be carried forward into the RPF's risk profile.
7. Each of the 5 mitigants sections provides for a Rating to be inserted by the supervisor. Individual questions or issues need not be rated. **ONLY ONE RATING IS TO BE PROVIDED FOR EACH OF THE 5 MITIGANTS SECTIONS.** These ratings will carry forward into the overall assessment of the quality of Controls/Mitigants/Compliance in the RPF as part of the overall ML/FT risk profile. Provision is also made for an overall supervisory rating of Controls/Mitigants at the end of the Questionnaire, composed subjectively of the ratings for the 5 mitigants sections. The overall rating is not an average but is based on supervisory judgement and on the materiality and degree of ML/TF risks being managed.

Risk Mitigants (risk management, controls, compliance, etc.)	Yes/ No	RPF's Description/Comments MANDATORY	Citation: Law, Regulation, etc.	For Board/Managing Partners Supervisors Use Only
A. Corporate Governance and Role of the Managing Partners/Directors				
General Policy		<p>RPF should provide a concise description and/or response to each of the applicable questions and mitigant areas covered.</p> <p>If “No” or not applicable, a description or justification is required.</p>		<p>Supervisor’s assessment/observations of the response to be concisely entered in this column.</p>
1.Has the Board/Managing Partners of Directors/Managing Partners formally established and implemented an AML/CTF policy and compliance program? Describe its main features and consistency with the AML/CTF legislation?				
2.How often are the policies and procedures reviewed and updated? Is there a policy on this?				
3.How does the RPF communicate, and ensure, that the AML/CTF program is effectively implemented by all relevant offices or units?				
4.How does the Board/Managing Partners supervise implementation of the AML/CTF program, including risk				

Risk Mitigants (risk management, controls, compliance, etc.)	Yes/ No	RPF's Description/Comments MANDATORY	Citation: Law, Regulation, etc.	For Board/Managing Partners Supervisors Use Only
management, and SAR reporting requirements?				
5.Has the Board/Managing Partners designated any of its members responsible for AML/CTF issues or created an AML/CTF Committee? If so when was the director or committee designated/established?				
6.What types of reports do the Board/Managing Partners and top management receive on implementation of the AML/CTF program? From whom and how often are such reports received?				
7.What types of arrangements are in place for the Board/Managing Partners to provide feedback/decisions to management and staff on reports it receives?				
8.Describe the reporting and communication arrangements with respect to AML/CTF between the Board/Managing Partners and the Independent Audit and Compliance functions as applicable.				
9.Describe the main features of the AML/CTF policy with respect to ML/TF risk identification, assessment				

Risk Mitigants (risk management, controls, compliance, etc.)	Yes/ No	RPF's Description/Comments MANDATORY	Citation: Law, Regulation, etc.	For Board/Managing Partners Supervisors Use Only
and the applicable policies, controls and procedures?				
10. Has the Board/Managing Partners formulated and communicated a code of conduct/ethics for directors, management and staff? Does it include AML/CTF issues?				
Management Information Systems (MIS)				
12. Does the MIS generate reports on ML/TF risks and trends of risk?				
13. Does the RPF have an information system capable of generating reports on customers, transactions and account activities for purposes of detecting, analyzing and reporting unusual and suspicious activities?				
14. Does the RPF maintain a customer database that can be used to ascertain the risk profile of customers? Are there specific customer reports that are generated e.g. on PEPs and other high risk customers? If so, is the database integrated into MIS?				
15. Do the management and the Board/Managing Partners receive				

Risk Mitigants (risk management, controls, compliance, etc.)	Yes/ No	RPF's Description/Comments MANDATORY	Citation: Law, Regulation, etc.	For Board/Managing Partners Supervisors Use Only
AML/CTF reports generated by the system or summaries thereof?				
Rating: A. Corporate Governance			Weak, Satisfactory, Strong	
Supervisor justification for Rating:				
B. Risk Management				
1. Is there a formal risk management policy (risk identification, assessment and control)? Does it include ML and TF risks?				
2. Is there a specialized Risk Management group or unit within the RPF? If so, do its functions include ML/TF risks?				
3. Are there policies and procedures for conducting periodic ML/TF risk assessments? If so what is the scope and frequency of such assessments?				
4. Does the RPF have an ML/TF risk classification or rating system in effect? If so, please describe.				
5. Has the RPF classified any customers, products and services, geographic exposures and delivery				

Risk Mitigants (risk management, controls, compliance, etc.)	Yes/ No	RPF's Description/Comments MANDATORY	Citation: Law, Regulation, etc.	For Board/Managing Partners Supervisors Use Only
channels in accordance with risk? How many are high risk? If so, state the underlying justification for such classification and provide a copy of the summary risk assessment results.				
6. Are there customers that are prohibited from doing business with the RPF based on risk of ML/TF? If so, which ones?				
7. Does the RPF have a screening mechanism for PEPs, Targeted Financial Sanctions or UN sanctioned persons/entities list, other official lists, internally generated lists of high-risk customers? What system and procedures are used for such classification and screening?				
8. Are there any specific risk controls to prevent the RPF from being used for purposes of Proliferation Finance?				
9. Are there any policies and procedures that take into account ML/TF risks in approving expansion of services and business lines including new				

Risk Mitigants (risk management, controls, compliance, etc.)	Yes/ No	RPF's Description/Comments MANDATORY	Citation: Law, Regulation, etc.	For Board/Managing Partners Supervisors Use Only
branches subsidiaries in domestically and abroad? Has the RPF identified/classified high-risk locations where it and its customers conducts business?				
10. What role if any do risk management staff, independent auditors and compliance function play in development of new product, business lines and geographic markets?				
Rating: B. Risk Management			Weak, Satisfactory, Strong	
Supervisor justification for Rating:				

Risk Mitigants (risk management, controls, compliance, etc.)	Yes/ No	RPF's Description/Comments MANDATORY	Citation: Law, Regulation, etc.	For Board/Managing Partners Supervisors Use Only
C. AML/CTF Policies and Procedures				
Customer Due Diligence (CDD/KYC)				
1. Does the RPF have formal implemented policies and procedures for CDD/KYC principles?				
2. Have the policies and procedures been disseminated to management and relevant employees? How is dissemination conducted?				
3. How often are the CDD policies and procedures reviewed? Updated?				
4. Are there specific CDD policies and procedures for risk rating customers? If so describe the rating system used. Is it correlated with the risk management policies? How?				
5. Are there specific CDD measures for certain customer categories. E.g. <ul style="list-style-type: none"> • Non-residents • Legal entities and arrangements • PEPs (domestic and foreign) • Charities/Non-profit organizations • Other categories of e.g. high risk clients. 				

Risk Mitigants (risk management, controls, compliance, etc.)	Yes/ No	RPF's Description/Comments MANDATORY	Citation: Law, Regulation, etc.	For Board/Managing Partners Supervisors Use Only
6.Are the same AML/CTF policies and procedures implemented across all offices and subsidiaries, domestic and foreign? If not, why?				
7.Do the CDD policies and procedures provide for: <ul style="list-style-type: none"> • Customer Acceptance/Rejection • Closure of accounts and business relationships • Risk-based CDD • Customer, account and transaction monitoring 				
8.Are there specific CDD policies and procedures for: <ol style="list-style-type: none"> a) Identifying and verifying beneficiaries/ultimate beneficiaries of clients and accounts? b) Recording information on the purpose and intended nature of the business relationship/transaction. c) Where applicable obtaining information on the source of funds and wealth. d) Updating customer records including risk profile. 				
9. Does the RPF's CDD policy include checking of clients against high-risk customers in official country lists or				

Risk Mitigants (risk management, controls, compliance, etc.)	Yes/ No	RPF's Description/Comments MANDATORY	Citation: Law, Regulation, etc.	For Board/Managing Partners Supervisors Use Only
lists issued by international organizations e.g. UN terrorism lists.				
10. Describe the RPF CDD procedures when customer business is conducted through or with the participation of: a) Third party intermediaries (e.g. lawyers and other professionals) b) Other non-face-to-face business.				
11. Are there and if so describe CDD procedures for transactions involving bearer share companies, nominee shareholder companies, companies held in trust or similar arrangements? How is beneficial ownership established and recorded?				
12. Are any CDD procedures outsourced? Does the RPF depend on CDD conducted by other parties, e.g. banks and related entities?				
Monitoring and Suspicious Activity Reporting				
1. Does the RPF have an internal system for monitoring, detecting and reporting unusual and suspicious				

Risk Mitigants (risk management, controls, compliance, etc.)	Yes/ No	RPF's Description/Comments MANDATORY	Citation: Law, Regulation, etc.	For Board/Managing Partners Supervisors Use Only
activities? Is it manual or automated? Describe.				
2. Are there specific monitoring systems for terrorism and proliferation finance? If so describe in detail.				
3. Does the RPF have a system for monitoring and reporting unusual and suspicious activity on a group-wide basis from offices and subsidiaries? What are the procedures with respect to foreign branches and affiliates reporting to head office?				
4. Describe the role of compliance officer/MLRO in SAR reporting.				
5. Describe, if any, the security measures applied to prevent information about unusual and suspicious activities from being disclosed to unauthorized parties internally and outside of the RPF				
6. Are monitoring mechanisms risk-based?				
7. Are there specific monitoring mechanisms for? a) PEPs				

Risk Mitigants (risk management, controls, compliance, etc.)	Yes/ No	RPF's Description/Comments MANDATORY	Citation: Law, Regulation, etc.	For Board/Managing Partners Supervisors Use Only
b) High risk foreign clients and cross-border transactions? c) Charities/NPOs d) Other client, account or transaction categories.				
8. What is the procedure applied once an account, transaction or activity is identified as unusual or suspicious? Are these procedures documented? How are they communicated to staff?				
9. Describe the analytical process that is undertaken to analyze unusual and suspicious activities.				
10. Describe the decision making process for determining whether or not to send an SAR to the FIA.				
11. Who has the final decision on whether to send a SAR to the FIA?				
12. How many SARs have been sent to the FIA in the past 3 years?				
13. Is there a policy to protect the employees, if they report suspicious transactions in good faith, e.g. from administrative, and legal liability and of their identity including within the RPF?				
14. Are there administrative sanctions for employees that do not adhere to				

Risk Mitigants (risk management, controls, compliance, etc.)	Yes/ No	RPF's Description/Comments MANDATORY	Citation: Law, Regulation, etc.	For Board/Managing Partners Supervisors Use Only
the monitoring and reporting policies and procedures? Have any been applied in the last 3 years?				
Record keeping				
1.Is there a records retention policy? If so describe.				
2.How long are customer identification and CDD, transactions, suspicious activity reports, etc. maintained?				
3.How are records maintained? Paper, electronically, onsite, offsite storage?				
4.How do records allow for tracing transactions and provide a clear audit trail? Has this system been tested? If so when and by whom?				
5.What are the security measures for recordkeeping?				
6.Describe the procedures for accessing and retrieving AML/CTF related data. How long would it take to retrieve the information for a particular customer going back 5 years if requested by the supervisor and other competent authorities? Has this been tested? If so when was it last done?				

Risk Mitigants (risk management, controls, compliance, etc.)	Yes/ No	RPF's Description/Comments MANDATORY	Citation: Law, Regulation, etc.	For Board/Managing Partners Supervisors Use Only
7. Have there been requests from the authorities (e.g. FIA) for customer data? What were the results with respect to ease of access by the authorities?				
8. Are there any secrecy, contractual, legal or fiduciary restrictions on the provision of information to competent authorities?				
9. Can the RPF obtain records relating to clients of foreign offices, subsidiaries and affiliates? Can such information include SAR related information? Describe in detail.				
Know Your Employee				
1. Does the RPF have an internal human resources policy and procedures that include measures to ensure the integrity of officers/employees?				
2. Does the RPF screen prospective employees, (e.g. criminal records, work experience, etc.)? If yes, what other checks and examinations does your company conduct?				
3. Describe the RPF's employee vacation policy. Is this policy applied				

Risk Mitigants (risk management, controls, compliance, etc.)	Yes/ No	RPF's Description/Comments MANDATORY	Citation: Law, Regulation, etc.	For Board/Managing Partners Supervisors Use Only
for AML/CFT controls? If so explain why and how it is applied.				
Rating: C. AML/CTF Policies and Procedures				Weak, Satisfactory, Strong
Supervisor justification for Rating:				
D. Independent Controls (System-Wide)				
Independent Audit				
1. Does the RPF have an Independent Audit Department/function? If so to whom does the independent auditor report?				
2. Is the audit function outsourced and if so describe?				
3. Does the independent audit review and test the AML/CTF program, CDD/KYC policies and procedures? Is there a specific AML/CTF audit plan?				
4. If 2 above is yes, how frequent is the review conducted? When was the last time there was an independent audit review AML/CTF? Describe the				

Risk Mitigants (risk management, controls, compliance, etc.)	Yes/ No	RPF's Description/Comments MANDATORY	Citation: Law, Regulation, etc.	For Board/Managing Partners Supervisors Use Only
scope of the last review and its findings.				
5. Has the Board/Managing Partners established an independent audit Committee to deal with audit matters? If so does the Committee deal with AML/CTF issue and how?				
6. What is the size of the independent audit function? What proportion of time is devoted to AML/CTF issues by the internal audit?				
7. Does the independent audit review the Compliance/MLRO function? When was it last reviewed? What were the findings?				
8. Is the independent audit function risk-based generally and with respect to AML/CFT? Are controls and compliance with high risk clients and business lines specifically reviewed e.g. PEPs, charities/NPOs, and other high-risk categories?				
9. Describe the system for dissemination of independent audit reports and recommendations. Do these reports include AML/CTF issues and does compliance directly receive such reports?				

Risk Mitigants (risk management, controls, compliance, etc.)	Yes/ No	RPF's Description/Comments MANDATORY	Citation: Law, Regulation, etc.	For Board/Managing Partners Supervisors Use Only
External Audit				
10. Is the external auditor legally required to review AML/CFT legal compliance and controls?				
11. Is the external audit risk-based and if so please describe and whether such approach covers AML/CFT?				
12. How much time and human resources does the external audit devoted to AML/CFT issues?				
13. Who are the main counterparties that the auditor interacts with on AML/CFT?				
14. Other than for legal compliance, does the external auditor's review the internal control environment AML/CTF controls? If yes, what were the findings and how were they communicated to management?				
15. Describe the main AML/CFT findings in the auditors last report/management letter and the action actually taken by management as a result.				
16. Does the auditor review AML/CFT issues on a consolidated				

Risk Mitigants (risk management, controls, compliance, etc.)	Yes/ No	RPF's Description/Comments MANDATORY	Citation: Law, Regulation, etc.	For Board/Managing Partners Supervisors Use Only
basis including foreign offices, subsidiaries and affiliates?				
17. How much was the auditor paid in the past 3 years?				
18. How many times has the auditor been changed in the past 5 years?				
19. On a scale of 1 to 3 with 1 being very good and 3 unsatisfactory, how satisfied is management with the AML/CFT work done by the auditors?				
Compliance Function/MLRO				
1. Has the Board/Managing Partners formally established a compliance function?				
2. Has the RPF appointed an AML/CTF compliance officer (CO) or MLRO)? If so provide the name, functions and position within the organization?				
3. To whom does the CO/MLRO report within the organization? Describe the reporting system and process for the CO.				
4. Are there specific qualification and experience requirements for the CO? If so provide details of the AML/CTF				

Risk Mitigants (risk management, controls, compliance, etc.)	Yes/ No	RPF's Description/Comments MANDATORY	Citation: Law, Regulation, etc.	For Board/Managing Partners Supervisors Use Only
CO's professional qualifications, training, duties and responsibilities.				
5.What's the budget of the compliance function and/or CO for the past 3 years? Who prepares and approves the budget for compliance?				
6. Who conducts the CO's periodic/annual performance evaluation? Who approves promotions and salary changes?				
7.Does each office, subsidiary or affiliate have a compliance officer? If so describe the relationship with the head office CO.				
8.Is there a Group compliance function? If so describe its relationship with the operating unit compliance officers.				
9.For RPFs with cross-border offices and subsidiaries, describe the compliance function and how it relates to the Head Office.				
10. Does the AML/CTF CO carry on duties other than AML/CTF? If so, what other functions and what proportion of time is devoted to AML/CTF compliance issues?				

Risk Mitigants (risk management, controls, compliance, etc.)	Yes/ No	RPF's Description/Comments MANDATORY	Citation: Law, Regulation, etc.	For Board/Managing Partners Supervisors Use Only
11. Provide copies of the last 3 reports prepared by the chief AML/CTF compliance officer.				
12. Describe the role of the AML/CTF compliance officer in (a) monitoring and reporting of suspicious activities; (b) training; (c) development of risk systems and controls, (d) other issues.				
Rating: D. Internal Controls (system-wide)				Weak, Satisfactory, Strong
Supervisor justification for Rating:				
E. Resources (Staff, Training, Other)				
1. Is there a specific annual budget allocated for AML/CFT? If so what was the budget for the past 3 years?				
2. Is there a specific AML/CFT training budget? If so what was the budget for the past 3 years?				
3. Is there an approved AML/CTF training programme in place for employees? Who approves?				
4. What type of AML/CTF training program (type, frequency, participants, etc.) has been implemented for employees? If any,				

Risk Mitigants (risk management, controls, compliance, etc.)	Yes/ No	RPF's Description/Comments MANDATORY	Citation: Law, Regulation, etc.	For Board/Managing Partners Supervisors Use Only
describe the program. When was the last training program delivered?				
5.Has the Board/Managing Partners and senior management participated in AML/CTF training? If so describe.				
6.Does the CO attend professional training regarding ML/TF methods and typologies, CDD, suspicious activity monitoring and reporting, recordkeeping etc.? Describe the training program for the CO and indicate the type of training received in the last 12 months.				
7.Please indicate whether any one or more of the following staff training was provided in the past 12 months: <ul style="list-style-type: none"> • Seminars and workshops • Self-directed • Computer-based • Other (please specify) 				
8.Is there a mechanism of ensuring that every employee requested to attend training actually attends the training?				
9.Are there different types of AML/CTF training programs e.g. for new and existing employees? By type of business activities, etc.				

Risk Mitigants (risk management, controls, compliance, etc.)	Yes/ No	RPF's Description/Comments MANDATORY	Citation: Law, Regulation, etc.	For Board/Managing Partners Supervisors Use Only
10. Does the RPF communicate to staff new AML/CTF laws/regs or changes to existing AML/CTF laws/regs, policies or procedures to employees?				
11. Does the RPF retain records of its training sessions including attendance records and relevant training materials used? If so provide copies. Are there consequences for not attending training programs?				
Rating: E. Resources (staff, training, other)			Weak, Satisfactory, Strong	