

**APPENDIX A**

**Cayman Islands Monetary Authority**

**SUMMARY OF PRIVATE SECTOR CONSULTATION AND FEEDBACK STATEMENT**



**GUIDANCE NOTES (Amendments) ON THE PREVENTION AND DETECTION  
OF MONEY LAUNDERING AND TERRORIST FINANCING  
IN THE CAYMAN ISLANDS**

**ASSESSING RISK & APPLYING A RISK BASED APPROACH**

	<b>Paragraph No.</b>	<b>Industry comment</b>	<b>Authority's response</b>	<b>Consequent amendments to the draft GN</b>
<b>Section B: The Risk Based Approach</b>  <i>"FSPs in conducting their risk assessments should take into account all relevant information from various sources including, but not limited to..."</i>	5	Requesting that wording be amended to read "FSPs in conducting their risk assessments should take into account relevant information from various sources <b>which may include but is not limited to...</b> " <b>or</b> "FSPs in conducting their risk assessments should take into account relevant information from various sources, <b>which might include some or all of the following non-exhaustive list.</b> "	Paragraph 5 will be amended as follows:  "FSPs in conducting their risk assessments should take into account all relevant information from various sources which may include but is not limited to."	Amended

<p><i>"FSPs in conducting their risk assessments should take into account all relevant information from various sources including, but not limited to:</i></p> <p><i>the NRA of other jurisdictions in which the FSPs have subsidiaries or customers"</i></p>	5 (2)	<p>Clarification is being sought on the extent of the expectation to obtain all such information. The requirement to obtain such information would be unduly burdensome and that requirement of Paragraph 5 (7) which states <i>"other credible and reliable sources that can be accessed individually or through commercially available databases or tools that are determined necessary by an FSP on a risk sensitive basis"</i> would reasonably address the requirements of paragraph 5(2).</p>	<p>The wording of paragraph 5 has been amended and factors listed in paragraph 5 (1) to (7) are not exhaustive.</p>	No amendment
<p><b>Section C:</b> <b>Identification and Risk Assessment</b></p> <p><i>"When identifying and assessing risk, FSPs should adopt risk assessment policies and procedures appropriate to their size, nature and complexity. ML/TF risks should be measured considering all available relevant information."</i></p>	1	<p>Requesting revision to the text as follows:  <i>"When identifying and assessing risk, FSPs should adopt risk assessment policies and procedures appropriate to their size, nature and complexity. ML/TF risks should be measured considering <del>all</del> relevant available relevant information."</i></p> <p>(The use of "all" is too prescriptive and finite and runs contrary to the first sentence which makes it clear that risk assessment has to be proportionate to a businesses' size, nature and complexity)</p>	<p>Paragraph 1 will be amended as follows:  When identifying and assessing risk, FSPs should adopt risk assessment policies and procedures appropriate to their size, nature and complexity. ML/TF risks should be measured considering all information that is relevant and available.</p>	Amended

<p><i>"FSPs should identify and assess the inherent and residual risks they face with regard to their products, services, delivery channels, customer types, geographic locations in which they or their customers operate and any other relevant risk category."</i></p>	2	<p>Requesting deletion – (This is a repeat of section B, paragraph 7- it is not identically worded so should be deleted for avoidance of confusion).</p>	<p>Paragraph 2 refers specifically to inherent and residual risks. Section B – paragraph 7 refers to the general requirements for FSPs to assess and identify ML/TF risks.</p>	No amendment
<p><i>"ML/TF risks may be measured using a number of risk categories and for each category applying various factors to assess the extent of the risk. For example, one of the risk factors that may be relevant when considering the risk associated with its customers whether a customer issues bearer shares<sup>1</sup> or has nominee shareholders."</i></p>	3	<p>I wouldn't necessarily associate nominee shareholders for example regulated financial institutions use nominees frequently.</p>	<p>Comment is unclear.</p>	No amendment
<p><i>"FSPs should make their own determination as to the risk weights to be given to the individual risk factors or combination of risk factors. When weighing risk factors, FSPs should take into consideration the relevance of different risk factors in the context of a particular customer relationship or occasional transaction. Examples of the application of various factors to the different categories that may result in high and low risk classifications are provided below. When weighting risk, FSPs should ensure that:</i></p> <p><i>(1) weighting is not unduly influenced by any one factor;</i></p> <p><i>(2) economic considerations do not influence the risk rating;</i></p> <p><i>(3) situations do not arise where it is not possible for any business relationship to be classified as high risk;</i></p>	5	<p>Paragraph 5 states Risk factors: the examples provided are useful but should be reviewed and amended periodically as risks evolve over time.</p>	<p>It is the duty of FSPs to regularly evaluate their risks and detect new/emerging risks and factor them in their risk assessment framework.</p>	No amendment

<sup>1</sup> Note that bearer shares are not permitted under the laws of the Cayman Islands.

<p>(4) situations which are identified by relevant legislation as always presenting high ML/TF risks, are not overruled by the FSPs weighting; and</p> <p>(5) FSPs are able to override any automatically generated risk score, where necessary."</p>				
<p>"FSPs may differentiate the extent of CDD measures, depending on the type and level of risk for the various risk factors. For example, in a particular situation, they could apply normal CDD for customer acceptance measures, but enhanced CDD for ongoing monitoring, or vice versa. Similarly, allowing a high-risk customer to acquire a low risk product or service on the basis of a verification standard that is appropriate to that low risk product or service, can lead to a requirement for further verification requirements, particularly if the customer wishes subsequently to acquire a higher risk product or service."</p>	6	<p>Paragraph is confusing - could give an example of simplified due diligence for low risk, standard due diligence for standard risk and enhanced due diligence for high risk. Monitoring is separate.</p>	<p>The wording of paragraph 6, is consistent with the FATF CDD Standards and the AMLRS.</p> <p>Please refer to Part IV, V and VI of the AMLRs for additional guidance on the CDD.</p>	No amendment
<p>"FSPs should document their risk assessment in order to be able to demonstrate their allocation of compliance resources, keep these assessments up-to-date and have appropriate mechanisms to provide risk assessment information to the relevant Supervisory Authority (and competent authorities and self-regulatory bodies ("SRBs"), if required). The nature and extent of any assessment of ML/TF risks should be appropriate to the nature, size and complexity of the business."</p>	7	<p>Not necessarily compliance in 3 lines of defence model and compliance being independent and advisory.</p>	<p>The comment is unclear.</p>	No amendment

<p><b>Section D- Risk Classification Factors</b></p> <p>"FSPs should consider the following high-risk factors when assessing customer risk with regard to..."</p>	4	<p>Please revise - FSPs <del>should</del> <b>could</b> consider the following high-risk factors when assessing customer risk with regard." (do not want to create a tick-box effect)</p>	The wording is suitable.	No amendment
<p><i>"FSPs should consider the following high-risk factors when assessing customer risk with regard ...the nature and behaviour of the customer."</i></p>	4 (3)	<p>I would not classify this as a high-risk factor as part of risk rating.</p> <p>This is a "red flag" which would probably warrant a SAR.</p>	<p>The high-risk factors listed in paragraph 4 (3) (a)to(i) are consistent with the AMLRs.</p> <p>Please refer to the FATF's RBA sector specific guidance for further information.</p>	No amendment
	4 (3) (b)	As above	Same response as provided for paragraph 4 (3)	No amendment
	4 (3) (d)	As above	Same response as provided for paragraph 4 (3)	No amendment
	4(3) (e)	As above	Same response as provided for paragraph 4 (3)	No amendment
	4(3) (f)	<p>As above</p> <p>Higher risk may just be – for example a client requests an unusual level of secrecy and is unable to provide rationale.</p>	Same response as provided for paragraph 4 (3)	No amendment
	4(3)(g)	As above	Same response as provided for paragraph 4 (3)	No amendment
	4 (3)(i)	This is a bit vague	The wording is suitable.	No amendment

<p><i>"When assessing customer risk, FSPs may consider the low-risk classifications for applicants / customers that satisfy the requirements under regulation 22 (d) of the AMLRs."</i></p>	5	<p>Same comment as fed back in AML3</p> <p>I would suggest leaving this open, otherwise a tick box compliance culture will arise (as per the legislation)</p> <p>It should be noted that large global organisations who employ as many staff as live in the Cayman Islands have large teams who compile these models on an annual and trigger event basis. This will not be sustainable for organisations here.</p> <p><b>IMPORTANT: Need to allow for already established models imposed by parent entities of global multinationals who would not be prepared to break their systems to accommodate the Cayman Islands only</b></p>	<ul style="list-style-type: none"> <li>- Comment unclear</li> <li>- FSPs per the AMLRs are expected to adopt an appropriate risk-based approach and comply with Cayman Islands legislation.</li> </ul>	No amendments needed
	7(1)	As above	Response same as provided for Section D - paragraph. 5.	No amendment
<p><i>"When identifying higher risks relating to country/geographic areas, FSPs should consider:</i></p> <p><i>whether the country is subject to sanctions, embargos or similar measures issued (e.g., sanctions imposed by the United Nations)"</i></p>	7(2)	<p>Paragraph 7 (2) states:</p> <p>Please delete:</p> <p>I would be careful here not to confuse sanctions with risk rating for AML."</p> <p>Sanctions should generally just be escalated as sanctions then investigated by a sanction's specialist</p>	Wording suitable as is.	No amendment
<p><i>"When identifying higher risks relating to country/geographic areas, FSPs should consider:</i></p>	7 (3)	Is this not already covered in point 1?	Paragraphs 7 (1) and (3) refer to two separate factors.	No amendment

<p><i>whether the country or geographic area has been identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their jurisdiction"</i></p>				
<p><i>In identifying lower risks relating to country/geographic areas, FSPs may consider:</i></p> <p><i>(1) countries identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT systems; and</i></p> <p><i>(2) countries identified by credible sources as having a low level of corruption or other criminal activity.</i></p>	8	<p>"Credible sources" must align with that term as proposed in the AMLR amendments.</p>	<p>The term "credible source" does not conflict AMLRs.</p>	<p>No amendment</p>
<p><i>"When identifying the risk associated with delivery channels, FSPs should consider the risk factors related to the extent that the business relationship is conducted on a non-face to face basis; and any introducers or intermediaries it utilises and the nature of those relationships."</i></p>	10	<p>Please re-word: "related to the extent that" does not make clear sense.</p>	<p>Wording amended as follows:</p> <p>When identifying the risk associated with delivery channels, FSPs should consider the risk factors related to the business relationship and/or occasional transaction conducted on a non-face to face basis; and any introducers or intermediaries it utilises and the nature of those relationships.</p>	<p>Amended</p>

<p><i>"When assigning high risk ratings relating to products, services and delivery channels, FSPs should consider:</i></p> <p><i>non-face-to-face business relationships or transactions (e.g. if the customer is not physically present for identification purposes, whether the FSP uses reliable forms of non-face-to-face CDD)"</i></p>	<p>11 (2)</p>	<p>Based on the international finance industry in the Cayman Islands, it seems unreasonable and not a proper use of the "RBA" for all non-face-to-face business to be immediately "high risk". Please delete this or make it clear that a high-risk designation is optional and is not prescriptive/automatic.</p> <p>(Given the nature of international work conducted through the Cayman Islands, this essentially negates any real value in a risk assessment for the vast majority of customers as they are all immediately high risk just because they are not here in person. This would result in huge administrative burdens which would damage our industry; this could also result in the genuine "high risk" customers not being properly identified and singled out as the real risk area for EDD.)</p>	<p>This wording is consistent with the AMLRS and FATF guidance.</p> <p>A proper risk based approach should consider all risk factors.</p>	<p>No amendment</p>
<p><i>"payments received from unknown or unassociated third parties."</i></p>	<p>11 (3)</p>	<p>Given the nature of international work conducted through the Cayman Islands, this essentially negates any real value in a risk assessment for the vast majority of customers as they are all immediately high risk just because they are not here in person. This would result in huge administrative burdens which would damage our industry; this could also result in the genuine "high risk" customers not being properly identified and singled out as the real risk area for EDD.</p>	<p>Response same as provided for Section D - paragraph. 11 (2)</p>	<p>No amendment</p>



<p><i>"Whether, in the case of insurance products/services, there is a surrender of single premium life product or other investment-linked insurance products with a surrender value"</i></p>	<p>11 (6)</p>	<p>Not sure what is meant by this?</p>	<p>This factor refers specially to the Insurance Industry.</p>	<p>No amendment</p>
<p><b>Section E: Risk Management and Mitigation</b></p> <p><i>"FSPs should establish their risk tolerance. Such establishment should be done by senior management and the Board. In establishing the risk tolerance, the FSP shall identify the risks that it is willing to accept and the risks that it is not willing to accept. It should consider whether it has sufficient capacity and expertise to effectively manage the risks that it decides to accept"</i></p>	<p>2</p>	<p>Please delete or soften this requirement to state that the risk assessment <u>may</u> result in a risk tolerance being formally established and documented.</p> <p>This also impacts the new requirement imposed by the Guidance Notes by paragraph 9F.</p> <p>(We understood from our review that a formal risk tolerance policy of this nature approved by senior management was not required by the MER and would not be practical in many scenarios. The Guidance envisages an extremely rigorous risk assessment process which will, where necessary, capture risk tolerances but having to decide and document up front what risks are to be accepted and which are not is very limiting and requires an element of predicting the future. A risk based policy should be able to consider each risk as it comes and apply the risk criteria on a case by case basis rather than imposing inflexible and blanket rules which could lead to governance breaches or issues and prevent the business being able to operate smoothly.</p>	<p>The successful implementation and effective operation of a RBA to AML/CFT depends on strong senior management leadership and oversight of the development and implementation of the RBA across the FSP.</p> <p><b>Senior management, together with the board, are responsible for setting up robust risk management and controls adapted by FSP's,</b> sound risk-taking policy; implement adequate mechanisms of internal communication related to the actual or potential ML/TF risks faced by the FSP. These mechanisms should link the board of directors, the AML/CFT chief officer, any relevant or specialised committee within the FSP (e.g., the risks or the ethics/compliance committee) the IT division</p>	<p>No amendment</p>

		The drafting of the Guidance Notes in these terms introduces onerous new obligations on all RFBs; these are not risk based and create obligations which as a matter of practice will be very onerous to all RFBs. It does not seem the creation of these obligations was the purpose of Guidance Notes (rather such obligations should be introduced by Regulations is required))	and each of the business areas; decide on the measures needed to mitigate the ML/TF risks identified and on the extent of residual risk the FSP is prepared to accept; and adequately resource the FSP's AML/CFT unit.	
<i>"The policies and procedures designed to mitigate assessed ML/TF/PF risks should be appropriate and proportionate to these risks and should be designed to provide an effective level of mitigation."</i>	6	Please delete – repeats 3 (c) (1)	Paragraph 6 requires "an effective level of mitigation."	No amendment
<i>"Some of the risk mitigation measures that FSPs may consider include:  (1) determining the scope of the identification and verification requirements or ongoing monitoring based on the risks posed by particular customers, products or a combination of both; (2) setting transaction limits for higher-risk customers or products; (3) requiring senior management approval for higher-risk transactions, including those involving PEPs; (4) determining the circumstances under which they may refuse to take on or terminate/cease high risk customers/products or services;</i>	8	Risk Mitigation: consider the use of data analytics to identify unusual patterns i.e. link and social network analysis, geographical spatial analysis, transaction timeline analysis, relationship mapping and activity heat maps.  8(3) and (5) Please delete one – they repeat each other in a confusing manner.	Noted  Paragraph 8 (3) delete.	Amended

<p>(5) <i>determining the circumstances requiring senior management approval (e.g. high risk or large transactions, when establishing relationship with high risk customers such as PEPs)."</i></p>				
<p>"<i>requiring senior management approval for higher-risk transactions, including those involving PEPs"</i></p>	<p>8 (3)</p>	<p>Depends on definition of senior management – not board...</p> <p>Not sure how higher risk transactions would be <i>identified</i> – <i>most banks would be screening for sanction indicators through wire transfer payments, this would have to break systems for this.</i></p>	<p>The onus is on FSPs to determine in accordance with the Guidance provided by the AMLRs and FATF what would be a considered a high-risk transaction for the purposes of their risk based assessments.</p>	<p>No amendment</p>
<p>"<i>Subsequent to establishing the risk mitigation measures, FSPs should evaluate their residual risk. Residual risk is the risk remaining after taking into consideration the risk mitigation measures and controls. Residual risks should be in line with the FSP's overall risk tolerance. Where the FSP finds that the level of residual risk exceeds its risk tolerance, or that its risk mitigation measures do not adequately mitigate high risks, the FSP should enhance the risk mitigation measures that are in place.</i>"</p>	<p>9</p>	<p>We appreciate the need to consider residual risk in the context of overall risk tolerance. It is suggested however, that the setting of risk tolerance cannot be separated from risk mitigation and controls and thus needs to consider residual risk before a risk tolerance is set- not after. As no transaction would be completely free of residual risk, even if such risk is low, we believe that the requirement should be that the risk tolerance is set to consider residual risk and risk tolerance simultaneously. For example, if one was to set the risk tolerance for PEPs, for instance, as low while having limited effective controls and numerous PEPs, then it would follow that the risk tolerance is set incorrectly and at odds with the institution's actual practices. We accept that an institution may change its tolerance and thus change its operating model-to-fit for instance, by</p>	<p>The Authority is not recommending a siloed approach to risk evaluation. The paragraph stresses risk controls that do not adequately mitigate risk to acceptable levels require further evaluation and action.</p>	<p>No amendment</p>

		off boarding PEPs, but the risk tolerance should in practice reflect an institution's actual state of affairs rather than serve as a goal. Otherwise, the risk tolerance would be undermined by practice.		
<p><b>Section F – Monitoring AML/CFT Systems and Controls</b></p> <p><i>"MONITORING AML/CFT SYSTEMS AND CONTROLS"</i></p>	Title	Please relabel title adding red text "Monitoring AML/CFT Risk and Its Impact on the Adequacy of Systems and Controls"	Wording is suitable.	No amendment
<p><b>Section G – New Products and Technologies</b></p> <p><i>"FSPs should have systems in place to identify and assess ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products such as:</i></p> <p><i>(1) digital information storage including cloud computing;</i></p> <p><i>(2) digital or electronic documentation storage;</i></p> <p><i>(3) electronic verification of documentation;</i></p> <p><i>(4) data and transaction screening systems; or</i></p> <p><i>the use of virtual or digital currencies"</i></p>	1	Perhaps clarify as there is no database such as Experian, is this referring to passport verification through for example Lexis Nexis?	Wording is suitable.	No amendment
"Systems utilizing new technologies that are involved with the collection, monitoring or	3	Not sure this adds anything?	Wording suitable as is.	No amendment

<p>maintenance of customer information for example, may not be as reliable or work as expected or may not be fully understood by staff. Such systems could therefore be vulnerable and result in FSPs not complying with the AMLRs."</p>				
<p><i>"FSPs should have policies and procedures in place or such measures as may be needed to prevent the misuse of technological development in ML/TF/PF schemes, particularly those technologies that favour anonymity. Banking and investment business on the Internet, for example, add a new dimension to FSPs' activities. The unregulated nature of the Internet is attractive to criminals, opening up alternative possibilities for ML/TF/PF, and fraud"</i></p>	5	Is this referring to Blockchain/crypto?	Reference is being made to all technological developments that may be used for AML/TF/PF purposes, not only blockchain/cryptocurrencies	No amendment
<p><i>"It is recognized that on-line transactions and services are convenient. However, it is not appropriate that FSP should offer on-line live account opening allowing full immediate operation of that account in a way which would dispense with or bypass normal identification procedures."</i></p>	6	The UK has allowed this – perhaps because of Experian which is not available here and where payments in and out are linked to the UK bank account.	This paragraph is consistent with the requirements of the AMLR that requires client identification as part of customer due diligence requirements. Please refer to AMLR 10 through 29.	No amendment
<p><b>Section I – Documentation</b></p> <p><i>"FSPs must document their RBA. Documentation of relevant policies, procedures, review results and responses should enable the FSP to demonstrate to the relevant Supervisory Authority and/or to a court: risk assessment systems including how the FSP assesses ML/TF/PF risks:</i></p> <p><i>risk assessment systems including how the FSP assesses ML/TF/PF risks"</i></p>	1(1)	Isn't necessarily a system.	The term "systems" as used in paragraph 1 (1) encapsulates all components of the risk assessment, which includes policies, procedures, controls etc.	No amendment

<p><i>"FSPs must document their RBA. Documentation of relevant policies, procedures, review results and responses should enable the FSP to demonstrate to the relevant Supervisory Authority and/or to a court: risk assessment systems including how the FSP assesses ML/TF/PF risks: how it monitors and, as necessary, improves the effectiveness of its systems and procedures"</i></p>	<p>1 (3)</p>	<p>Control is preferred when talking about risk, the control may be the procedure/checklist/system etc...</p>	<p>Response same as provided for Section I- paragraph. 1.</p>	<p>No amendment</p>
<p><b>Section J: Review of Risk Assessment</b></p> <p><i>"The AML/CFT risk assessment should be subjected to regular reviews to ensure that it adequately reflects the ML/TF risks pertaining to the FSP. FSPs should also assess information obtained as part of their ongoing monitoring business relationships and consider whether this affects the risk assessment. It is the expectation of the Monetary Authority that these reviews are approved by the Board of the FSP"</i></p>	<p>1</p>	<p>Requesting that "periodic review should be conducted by an independent and qualified external party" and the</p> <p>Requesting revision of paragraph 1 to read - "The AML/CFT risk assessment should be subjected to regular reviews to ensure that it adequately reflects the ML/TF risks pertaining to the FSP. FSPs should also assess information obtained as part of their ongoing monitoring business relationships and consider whether this affects the risk assessment. It is the expectation of the Monetary Authority that these assessments are reviewed for awareness of risks by the Board of the FSP. (While the Board may review the risk assessment, it is suggested that an 'approval' should not be required)</p>	<p>Paragraph will be amended as follows:</p> <p>The AML/CFT risk assessment should be subjected to regular reviews to ensure that it adequately reflects the ML/TF risks pertaining to the FSP. FSPs should also assess information obtained as part of their ongoing monitoring business relationships and consider whether this affects the risk assessment. It is the expectation of the Monetary Authority that these reviews are approved by Senior Management and the Board of the FSP."</p>	<p>Amended</p>