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

Guidance Notes on the Prevention and Detection of Money Laundering, Terrorist Financing and Proliferation Financing in the Cayman Islands of 5 June 2020 with e-KYC and remote CDD/ongoing monitoring provisions.

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | **GENERAL COMMENT** | | | |
| **1.** | This consultation paper raises the topic of e-KYC service providers and provides examples (at page 12) of such providers in other jurisdictions (i.e., other than Cayman Islands). Could the Authority please confirm whether there is/will be: (i) a list of specific Digital ID systems approved for use by the Authority; and/or (ii) an approved Cayman-based Digital ID system?<br><br>YOTI, for example, is an approved E-ID / KTC service provider based in Jersey (a relevant case study is available at: https://www.yoti.com/wp-content/uploads/Jersey_case-study.pdf) that has been approved for use by the UK Government (https://www.yoti.com/blog/yoti-uk-government-approved-dbs-right-to-work-rent-checks/). | | The Authority does not prescribe or endorse the utilisation of any particular digital ID system or technology solutions. This should be taken in the context of the size of the FSP and the complexity of its activities. | No amendment required. |
| **2.** | All references to "laws" change to "Acts" | | All references to "Laws" changed to "Acts" throughout the document as per Citation of Acts of Parliament Law, 2020 (Law 56 Of 2020) | Amended as recommended |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| **3.** | The phrase "levels of assurance" is used throughout the guidance. CIMA should consider defining what this means and their expectations on FSP's obtaining such. | | The Authority agrees to the proposed need for clarity on the definition of "level of assurance " | **New Footnote 13 added, and reads as follows:**<br><br>"Assurance levels measure the level of confidence and accuracy in the reliability and independence of a digital ID system and its components." |
| | **SECTION SPECIFIC COMMENTS** | | | |
| **4.** | **Part II – General AML/CFT Guidance**<br>**Section 3 B (7)**<br>As a part of the RBA, FSPs should:<br>(1) identify ML/TF risks relevant to them;<br>(2) assess ML/TF risks in relation to:<br>(a) their applicants/customers (including beneficial owners);<br>(b) Country or geographic area in which persons under (a) above reside or operate and where the FSP operates;<br>(c) products, services and transactions that the FSP offers; and<br>(d) their delivery channels, including remote onboarding and ongoing | This amendment is to an existing list of risks which an FSP is required to assess as part of the RBA. 'Ongoing monitoring of business relationships' is a procedure adopted by FSPs to monitor risk on an ongoing basis and is not a risk in and of itself. Further, introducing a new requirement to risk assess 'ongoing monitoring of business relationships' is not related to e-KYC or digital onboarding, so is outside the scope of the Consultation Paper. On this basis, we do not consider that this wording should be included in the amendments to (d).<br>Our suggestion is that this wording is removed.<br>Suggested re-wording:<br>"(d) their delivery channels, including remote onboarding." | The Authority notes the proposed amendment; however, whilst it is agreed that ongoing monitoring is not a risk in and of itself, the requirement to conduct ongoing monitoring of business relationships is a necessary part of an RBA. Therefore, the Authority is of the opinion that where digital ID systems and/or other technologies are used, any risks surrounding their use should be considered, even in instances of the ongoing monitoring of business relationships.<br><br>Conducting ongoing monitoring is essential for FSPs to maintain an | **Part II – General AML/CFT Guidance Section 3 B (7), revised to read as follows;**<br>As a part of the RBA, FSPs should:<br>(1) identify ML/TF risks relevant to them;<br>(2) assess ML/TF risks in relation to:<br>(a) their applicants/customers (including beneficial owners);<br>(b) Country or geographic area in which persons under (a) above reside or operate and |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | monitoring of business relationships. | | understanding of a customer and the business relationship, keep CDD up-to-date, review and revise risk assessments as appropriate, and identify and report unusual transactions and activities. Ongoing monitoring is not a customer-driven rule but rather a transaction-driven rule.<br><br>This measure requires the FSP to assess the ML/TF risk related to the onboarding and monitoring of business relationships using remote, non-face-to-face means. For example, in the case of ongoing monitoring, a transaction may be flagged for falling outside of a customer's expected activity, and the client may be required to provide information and supporting evidence. The FSP may or may not permit this to be done remotely, in accordance with a risk-based approach. | where the FSP operates;<br>(c) products, services and transactions that the FSP offers; and<br>(d) their delivery channels, including remote onboarding and ongoing monitoring of business relationships. |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | 1.(2)(d) The ongoing monitoring of business relationships is a different concept; therefore, clause (d) should stop with the word "onboarding".<br><br>Or is it the intent of the Authority to include that the terminology monitoring is referring to updating or review of documents? | Please see the response provided above. | No further amendment required. |
| | | The inclusion of ongoing monitoring of business relationships in this way is misleading implying that ongoing monitoring is a risk.<br><br>If ongoing monitoring is intended to be one of the tasks that the FSP should do, it is already covered in the GN in Part II section 16. There is no need to mention it anew as there are 45 different instances of the same in the GN.<br><br>The definition or remote onboarding appears multiple times in this revision. it adds volumes to an already complex document.<br><br>**Suggested amendment:**<br><br>Recommend removing the inserted language "..including remote onboarding4 and ongoing monitoring of business relationships…." | Please see the response provided above.<br><br>To add further clarity, ongoing monitoring is not a risk, but conducting ongoing monitoring remotely can be a risk; the degree to which it is based on the factors presented will be determined by the FSP. | No further amendment required. |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | Recommend amending the footnote to direct readers to the definition of Non face to face, and modifying non face to face to include the definition of remote onboarding. | | |
| | | Operational benefit to licensee to take a Risk Based Approach to remote onboarding and ongoing monitoring of business relationships.<br><br>Our reading of the definition of "remote onboarding" is that it appears to cover the following situations;<br>(a) the use of automated remote customer onboarding solutions; and<br>(b) the use of remote onboarding with human intervention (e.g., via email).<br><br>Is that the proposed intention of the Authority? | Remote onboarding covers both situations as the human intervention (eg. email) listed in example (b) is considered technology.<br><br>The Authority is satisfied that the definition of remote onboarding is sufficient, as provided for in **Footnote 9**. | No further amendment required. |
| **5.** | **Part II – General AML/CFT Guidance**<br>**Section 3 B (7) (2) (d)**<br>"their delivery channels, including remote onboarding and ongoing monitoring of business relationships. | There is a formatting error in Section 3 B (7)(2)(d). It currently reads:<br>(d) their delivery channels8, including remote onboarding9 and ongoing monitoring of business relationships.<br>The reference to Footnote 9 should be in superscript. Please note that this is only an issue in the Guidance | The proposed edit has been addressed by the Authority. | No further amendment required. |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | Notes and not in the Private Sector Consultation Paper ("PSCP"). | | |
| **6.** | **Section 1.I (4)** | Give consideration to the fact that website links may have changed over time. | The website link has been updated to he align with the current COG website. | **Section 1.I (4)**, website link updated to :<br><br>http://www.pola.gov.ky/portal/page/portal/plghome/publications/summary-results-of-the-mltf-national-risk-assessment-nra |
| **7.** | **Part II – General AML/CFT Guidance**<br>**Section 3 C (7)**<br>Customer identification and verification methods should align with the FSP's risk assessment of the client so the decision to onboard a customer remotely, using e-KYC methods and digital ID technologies is on a case by case basis, dependent on the risks presented and assessed." | In Provision 7, the suggested approach to rely and apply e-KYC methods/ digital ID technologies on a client-by-client risk basis is not a sustainable approach for an FSP that has performed a risk assessment to assess the suitability and appropriateness of that digital ID system given the nature of its business and understanding of its customer portfolio, including customer type(s), geographical location and availability of independent, reliable data sources.<br><br>The FATF (2020), Guidance on Digital Identity has outlined recommendations for government authorities [Provision 20] to "encourage a flexible, risk-based approach to using digital ID systems for CDD that supports financial inclusion. Consider providing guidance on how to use digital ID | The Authority agrees to the proposed amendment for clarity. | **Part II – General AML/CFT Guidance**<br>**Section 3 C (7) revised to read as follows:**<br><br>"Customer identification and verification methods should align with the FSP's risk assessment of its ~~client~~ **customers**, so the decision to onboard a customer remotely, using e-KYC methods and digital ID technologies, ~~is on a case by case basis~~, should be dependent on the risks presented and assessed~~.~~**, and where applicable consider the application of tiered CDD**." |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | systems with different assurance levels for identity proofing/enrolment and authentication for tiered CDD."<br><br>**Suggested amendment:**<br><br>"Customer identification and verification methods should align with the FSP's risk assessment of its clients, so the decision to onboard a customer remotely, using e-KYC methods and digital ID technologies, should be dependent on the risks presented and assessed, and, where applicable consider the application of tiered CDD." | | |
| | | In the second sentence of new Provision 7, the word ''client'' has been used. Elsewhere in Section 3C, the word ''customer'' has been used. We would suggest replacing ''client'' with ''customer'' to ensure consistency in usage. | The Authority notes this comment on the use of the term "client". The section will be updated to utilise the term "customer" throughout for consistency.<br><br>Please see the above amendment. | No further amendment required. |
| | | It is clear that a case-by-case assessment is required at onboarding for using e-KYC methods and digital ID technologies, however, is it possible to use a more widespread application of e-KYC | The GNs do not preclude an FSP from using e-KYC methods and digital ID technologies for remediation and ongoing monitoring in the absence | No further amendment required. |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | methods/digital ID technologies for remediation and ongoing monitoring subject to not identifying any higher risk characteristics which might suggest this is not appropriate? | of the identification of higher risk characteristics. | |
| | | There is conflict between 7 and 8. 7 says the decision to use EKYC should be made on case by case basis, dependent on the risks presented. Should it not simply say methods chosen to complete KYC should be appropriate for the risks. This is the same regardless of whether its E KYC or Digital or other means.<br><br>In truth, retaining this section creates a redundancy of the language in Section 3C6.<br><br>Recommend removing the inserted language as its redundant with the language in Section 3C6.<br><br>The suggested approach to rely and apply e-KYC methods/ digital ID technologies on a client-by-client risk basis is not a sustainable approach for an FSP that has performed a risk assessment to | The new guidelines provide guidance on the use of e-KYC/ digital ID technologies, not on CDD methods generally.<br><br>**Section 3 C (6)** speaks to FSP's differentiating the extent of CDD measures, depending on the type and level of risk for the various risk factors. **New provision 8** supports this by requiring additional verification to complement the e-KYC measures if there is a higher level of risk. | No further amendment required. |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | assess the suitability and appropriateness of that digital ID system given the nature of its business and understanding of its customer portfolio, including customer type(s), geographical location and availability of independent, reliable data sources.<br><br>The FATF (2020), Guidance on Digital Identity has outlined recommendations for government authorities [Provision 20] to ""encourage a flexible, risk-based approach to using digital ID systems for CDD that supports financial inclusion. Consider providing guidance on how to use digital ID systems with different assurance levels for identity proofing/enrolment and authentication for tiered CDD."<br><br>There should be clarification around using e-KYC on a widespread application basis. It would not be feasible to apply digital technology to some and not to others. Which goes back to the definition of the E-KYC definition. Similar to existing methods, if doubts about the | | |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | veracity of the identification exist, further verification would be necessary, in accordance with the risk assessment.<br><br>The amendments state for higher risk ML/TF, the FSP should conduct additional verification measures to ensure the accuracy of e-KYC procedures. Can the guidance notes include examples of an additional verification measure, should the additional verification be performed within the e-KYC system/ procedure or can it be performed outside of the e-KYC?<br><br>**Suggested amendment:**<br><br>Customer identification and verification methods should align with the FSP's risk assessment of its clients, so the decision to onboard a customer remotely, using e-KYC methods and digital ID technologies, should be dependent on the risks presented and assessed, and, where applicable consider the application of tiered CDD. | | |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | In line 2, there should be a semicolon after the word "client" and the word "so" deleted and replaced with the word: therefore". In line 3, the word "required should be replaced with the words "to be made". Also in line 3, the word "dependent" should be replaced with the word "depending". | | |
| **8.** | **Part II – General AML/CFT Guidance**<br>**Section 3 C (8)**<br>"Where the customer, product, service, or jurisdiction is identified as<br>higher risk for ML/TF, the FSP should conduct additional verification<br>measures to ensure the accuracy of e-KYC procedures. The FSP may also<br>consider not using e-KYC or remote onboarding for the establishment of<br>the business relationship or for performing ongoing CDD but reverting to<br>face-to-face interactions or reviewing original certified documents, for<br>example." | The Authority has explained that FSPs ''should conduct additional verification measures to ensure the accuracy of e-KYC<br>procedures''. This should be clarified to confirm whether FSPs need to conduct additional verification measures to ensure the accuracy of: (i) e-KYC procedures (e.g., internal policies); (ii) the accuracy of identification being provided; or (iii) the accuracy of the e-KYC system being used. | The Authority notes that failure to utilize e-KYC or remote onboarding measures would necessitate FSPs to revert back to face-to-face meetings and hard copy submissions of certified documents.<br><br>Moreover, additional verification measures are to ensure that the FSP has:<br><br>1. Identified and verified the customer's identity using reliable, independent source document, data or information in accordance with ***Regulation 12 (1) (a)*** of the **AMLRs**. | No amendment required. |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | | 2. Furthermore, it guarantees FSPs have satisfied ***Regulation 20***, which speaks to the evidence of the identity being satisfactory if it reasonably establishes that the applicant for business is the person the applicant for business claims to be. | |
| | | The FATF (2020), Guidance on Digital Identity has outlined recommendations for government authorities [Provision 20] to "encourage a flexible, risk-based approach to using digital ID systems for CDD that supports financial inclusion. Consider providing guidance on how to use digital ID systems with different assurance levels for identity proofing/enrolment and authentication for tiered CDD."<br><br>**Suggested amendment:**<br><br>"Where the customer, product, service, or jurisdiction is identified as higher risk for ML/TF, the FSP should conduct additional verification measures to ensure the accuracy of e-KYC procedures. The | Please see the response provided above. | No amendment required. |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | FSP should consider a tiered CDD approach to mitigate ML/TF risks." | | |
| | | Clarify "the FSP should conduct additional verification measures to ensure the accuracy of e-KYC procedures". FATF Guidance on Digital Identity states that customer identification measures that rely on reliable, independent digital ID systems, with appropriate risk-mitigation measures in place, may be standard risk, and may even be lower risk (Para 25). A focus on "verifying the accuracy" of the digital ID measures maybe misleading. Would want to avoid the need to gather physical documents outside of a digital system with multi-layered high level assurances and an in-built (systems-based) tiered approach.<br><br>Perhaps better wording would be "the FSP should conduct additional due diligence measures commensurate to the higher risks posed"? As per the FATF Guidance on Digital Identity, emphasis should be on testing assurance levels and systems-based analysis. | Please see the response provided above.<br><br>For further clarification, please also refer to **Section 3 D (13) and (14).** | No amendment required. |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | There should be no need to re-evaluate the accuracy of EKYC procedures each time the FSP decides to make use of E KYC methods and digital ID. The initial assessment of the risks and the resulting procedures should be enough in much the same way as any other method used to complete the KYC process.<br><br>The second sentence is redundant with the language in Section 3C6.<br><br>Recommend removing the inserted language as its redundant with the language in Section 3C6. | Please see response provided above.<br><br>For further clarification, please also refer to **Section 3 D (13) and (14).** | No amendment required. |
| | | This comment suggests if any of the individual risk parameters are high risk additional verification measures should be undertaken. However, this does not take into consideration that the overall risk rating of the customer may not be high risk, notwithstanding the high risk factor rating.<br><br>This should only be taken into consideration if the customer is high risk. It seems illogical that if the product, service or jurisdiction risk factor is rated as high risk additional identification verification procedures would be required to be | A customer with high risk factors would not be considered low risk. If mitigating measures have been applied, the risk rating may be reduced to medium high or medium but never low. A risk rating of a customer does not exist in isolation. It is an accumulation of the all the relevant risk factors associated with the customer.<br><br>Further, as stipulated in **Regulation 12 of the** | No amendment required |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | performed on the customer whose customer risk factor rating is low.<br><br>This amendment suggests that e-KYC or remote onboarding should not be used if a higher risk is identified and that original certified documents are a better method of verification than digital ID technologies. This comment also implies "original" certified documents should be obtained – this is reverting back to the old approach. There is a request to remove this as it is creating a higher standard than what is currently being done, dictating enhanced due diligence which is already covered in the guidance notes.<br><br>If the risk rating is elevated for reasons such as PEP, or jurisdiction, additional verification on the identity of the individual is not necessary as it is not the identity of the person that raises the risk. Any additional verification that is conducted should address the specific risk, as in more information on SOF in cases of PEPs. The higher risk does not negate the veracity of the digital ID process as this clause suggests. | **AMLRs**, FSPs are also required to collect additional information to assist in verifying the customer's identity when establishing the business relationship at onboarding, authenticate the identity of customers, determine the customer's business risk profile and conduct ongoing due diligence on the business relationship. | |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | At the end of line 4, the word "reverting" should be followed by a comma and then the words "for example,". The words "for example" at the end of line 5 should be deleted.<br><br>It is the position of some members that digital verification is more reliable than 'certified documents". In line with a risk based approach, the FSP should determine what can be relied upon as it relates to verification. | | |
| **9.** | **Part II – General AML/CFT Guidance**<br>**Section 3 D (13)**<br>"FSPs should consider the basic components of digital ID/e-KYC[5] systems and take an informed risk-based approach to relying on these when conducting non-face to face onboarding or ongoing monitoring of business relationships. This includes understanding a chosen system's assurance levels and ensuring that those levels are appropriate to the assessed money laundering/terrorist financing risks of the scenarios/cases to which the system is being used. FSPs must ensure the level of assurance is adequate for the jurisdiction, product, customer etc." | The Authority should provide additional guidance on assessing assurance levels and assessing the suitability of digital ID systems to the industry. Consider leveraging the FATF Standards, which are technology-neutral and are outlined in the FATF (2020), Guidance on Digital Identity [p. 10 Figure 1] and Section V: ASSESSING WHETHER DIGITAL ID SYSTEMS ARE SUFFICIENTLY RELIABLE AND INDEPENDENT UNDER A RISK-BASED APPROACH TO CDD<br><br>The FATF (2020), Guidance on Digital Identity recommends that countries consider its approach in establishing their own digital ID | The Authority agrees with the proposed amendment and will add a footnote which includes a definition of assurance levels and further guidance on assessing assurance levels and the suitability of digital ID systems.<br><br>The Authority expects that once the FSP is satisfied that it knows the assurance levels of the digital ID system, it should analyse whether the digital ID system is adequate, in the context of the relevant illicit financing risks, under a risk-based approach to | **New footnote 13 added, and read as follows:**<br><br>"Assurance levels measure the level of confidence and accuracy in the reliability and independence of a digital ID system and its components." |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | assurance frameworks and other relevant technical standards. | CDD. In other words, given the assurance level/s, is the digital ID system appropriate for use in customer identification/verification and ongoing due diligence in light of the potential ML/TF risks associated with the customer, products and services, and geographic area of operations.<br><br>For additional guidance on athe ssessment of Risk and applying a risk based approach, FSPs should refer to **Section 3 D (13) and (14)** of these Guidance Notes. | |
| | | In the sixth sentence of new Provision 13, the words ''money laundering/terrorist financing'' are used. Elsewhere in **Section 3D**, the abbreviation ''ML/TF'' is used. We would suggest using ''ML/TF'' throughout to ensure consistency in usage.<br><br>Consider including the words "the technology solution, including" after the words "the basic components of". | The Authority notes and agrees to the proposed amendments for consistency. | **Section 3 D (13) amended to read as follows:**<br>FSPs should consider the basic components of **the technology solution, including** digital ID/e-KYC systems and take an informed risk-based approach to relying on these when conducting non-face-to-face **remote** onboarding or ongoing monitoring of business relationships. This |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | Consider replacing the words "jurisdiction, product, customer etc" with the words "risk factors".<br><br>CIMA should consider clarifying that risk-based approach in this provision relates to technology solutions and not the customer. | | includes understanding a chosen system's assurance levels and ensuring that those levels are appropriate to the assessed ~~money laundering/terrorist financing~~ **ML/TF** risks of the scenarios/cases to which the system is being used. FSPs must ensure the level of assurance is adequate for the jurisdiction, product, customer and other relevant risk factors. |
| | | The Authority should provide additional guidance on assessing assurance levels and assessing the suitability of digital ID systems to the industry. Consider leveraging the FATF Standards, which are technology-neutral and are outlined in the FATF (2020), Guidance on Digital Identity [p. 10 Figure 1] and Section V: ASSESSING WHETHER DIGITAL ID SYSTEMS ARE SUFFICIENTLY RELIABLE AND INDEPENDENT UNDER A RISK-BASED APPROACH TO CDD.<br><br>The FATF (2020), Guidance on Digital Identity recommends that | The term "assurance level" refers to the level of trustworthiness or confidence in the reliability of each of the components of the digital ID process. This means having confidence that the digital ID system works as it is intended to and produces accurate results. (This should be subject to regular testing). The ID system should be adequately protected against internal or external manipulation or falsification, to fabricate or | No further amendment required. |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | countries consider its approach in establishing their own digital ID assurance frameworks and other relevant technical standards.<br><br>We noted that the Jersey Financial Services Commission regulations include the following: "In order to adequately consider the risks associated with E-ID, the licensee's Board/senior management should clearly identify, fully understand and document what the E-ID application does and does not do. For example: › is it to be used only to collect information about an individual (finding out identity)? › is it to be used to obtain evidence of that individual's identity? › is it to be used to collect more general relationship information about an individual from that individual, e.g. source of funds? › is it to be used to collect information about an individual from reliable and independent data sources? If so, where do these data sources originate and have they been assessed as to their reliability and/or independence?<br><br>**Source: Handbook for the prevention and detection of money laundering, the countering of terrorist** | create false identities or authenticate unauthorised users, including by cyberattack or insider malfeasance.<br><br>Additionally, the Authority expects that once the FSP is satisfied that it knows the assurance levels of the digital ID system, it should analyse whether the digital ID system is adequate, in the context of the relevant illicit financing risks, under a risk-based approach to CDD. In other words, given the assurance level/s, is the digital ID system appropriate for use in customer identification/verification and ongoing due diligence in light of the potential ML/TF risks associated with the customer, products and services, geographic area of operations. | |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | **financing, and the countering of proliferation financing** https://www.jerseyfsc.org/media/6263/section-4-identification-measures-finding-out-identityand-obtaining-evidence.pdf<br><br>We recommend the Authority consider similar guidance to be integrated into section 3 D. This is also covered in vendor due diligence.<br><br>In line 5, the word "to" should be replaced with "for". | | |
| **10.** | **Part II – General AML/CFT Guidance**<br>**Section 3 D (13) and (14)**<br>"13. FSPs should consider the basic components of digital ID/e-KYC systems and take an informed risk-based approach to relying on these when conducting non-face to face onboarding or ongoing monitoring of business relationships. This includes understanding a chosen system's assurance levels and ensuring that those levels are appropriate to the assessed money laundering/terrorist financing risks of the scenarios/cases to which the system is being used. FSPs must ensure the level of assurance is | We agree with the requirement to carry out risk assessments on new e-KYC/digital ID technology.<br><br>We suggest that the same should be built into the outsourcing risk assessment, so that when an FSP outsources its onboarding procedures, that the FSP should have to risk-assess the outsource service provider's digital ID/e-KYC systems (or rely on a risk assessment already performed by the outsourced service provider). | The Authority expects FSPs to undertake a risk assessment of the service provider and outsourcing arrangement.<br><br>Outsourcing should be in accordance with the principles set out in ***Section 10 C*** of the Guidance Notes.<br>For further guidance on outsourcing, FSPs may refer to the ***Statement of Guidance on Outsourcing*** issued by the Authority, where applicable. | No amendment required. |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | adequate for the jurisdiction, product, customer etc.<br><br>14. FSPs should carry out formal risk assessments of new e-KYC/digital ID technology which include documented consideration of how the proposed system works, the level of assurance that it provides, and any particular risks associated with it." | The risk assessment of technology solutions is inaccurately categorized in the Section 3D. It should be in 3E which is the risk management and mitigation. This is essentially what EKYC and digital ID solutions are. They are tools used to mitigate the risks associated in the client onboarding process.<br><br>**Suggested amendment:**<br><br>Transfer all relevant paragraphs being proposed here to the correct section in the GN, namely Section 3E. | **Section 3 D of Part II** of the Guidance Notes provides details on the classification and assessment of risk factors by FSPs using credible and reliable sources, as su,ch the Authority is of the view that **Provisions (13) and (14)** are not inaccurately categorised as they address risk assessment of new technological solution . | o further amendment required. |
| **11.** | **Part II – General AML/CFT Guidance**<br>**Section 3 D (14)**<br>**"**FSPs should carry out formal risk assessments of new e-KYC/digital ID technology which include documented consideration of how the proposed system works, the level of assurance that it provides, and any particular risks associated with it." | The Authority should provide additional guidance on assessing assurance levels and assessing the suitability of digital ID systems to the industry. Consider leveraging the FATF Standards, which are technology-neutral and are outlined in the FATF Guidance on Digital ID [p. 10 Figure 1] and Section V: ASSESSING WHETHER DIGITAL ID SYSTEMS ARE SUFFICIENTLY RELIABLE AND INDEPENDENT UNDER A RISK-BASED APPROACH TO CDD.<br><br>The FATF Guidance on Digital ID recommends that countries consider its approach in establishing their own digital ID assurance | Please see the response provided above relating to assurance levels. | No futher amendment required. |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | frameworks and other relevant technical standards. | | |
| | | This language is already largely accounted for under Section 3G. There is no need to explicitly mention eKYC digital id or video conference unless you would like to give them as examples in G.<br><br>**Suggested amendment:**<br><br>Delete paragraph or roll examples into Section.<br>3G.<br>We suggest adding risk factors to consider but the list would not be exhaustive:<br><br>For example, some risk factors to consider:<br>> accuracy of the underlying information and/or technology<br>> appropriateness of the application for the licensee's client base (i.e. some applications are aligned to verify identification within a specific region)<br>> timeliness of the applications' updates (i.e. sanctions lists)<br>> evaluation of the cyber security measures of the application<br>> storage of personal information" | The Authority is of the view that the purpose of this subsection is befitting under the heading of 'Risk Assessment of Technology Solutions'.<br><br>Further, the Authority agrees to amend the section and incorporate the examples of risk factors in the section | **Section 3 (14)** amended to read as follows :<br><br>" FSPs should carry out formal risk assessments of the new technology solution, including e-KYC/digital ID technology which include documented consideration of how the proposed system works, the level of assurance that it provides, and any particular risks associated with it, ***inter alia*****, accuracy of the underlying information and/or technology, appropriateness of the application for the licensee's client base (i.e. some applications are aligned to verify identification within a specific region),timeliness of the applications' updates (i.e. sanctions lists),evaluation of the cyber security measures of the application ,storage of** |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | This is also covered in vendor due diligence rather than risk assessment. | | **personal information, etc.** |
| **12.** | **Part II – General AML/CFT Guidance**<br>**Section 3 D (15)**<br>"The use of video-conferencing, as with other forms of non-face-to-face measures must be in accordance with a risk-based approach. FSPs should put in place appropriate controls during the video-conferencing process to verify the identity and authenticity of the ID documents presented. If an introducer or suitable certifier has met the customer, they must confirm to the FSP that they have met the customer via video-conferencing, including a photograph or scanned copy of the documents" | We do not think including the word 'introducer' here is appropriate, as an introducer would not be able to make the required confirmations to the FSP. Our suggestion is that this wording is removed.<br><br>**Suggested amendment:**<br><br>"If a suitable certifier has met the customer, they must confirm to the FSP that they have met the customer via video conferencing, including a photograph or scanned copy of the documents."<br><br>Consider including the word "certified" after the words "or scanned".<br><br>Consider including the words "of the customer" after the words "including a photograph". | According to the GN, an "Eligible Introducer" means a person that "introduces' applicants for business to an FSP and who satisfies the conditions set out in **Regulation 25** of the **AMLRs** and provides a written assurance pursuant to **Regulation 24(2)(b).**<br><br>The Authority's expectation is that an FSP must carry out appropriate due diligence on the introducer to ensure their eligibility and that written undertakings are received from the introducer in accordance with the Guidance Notes.<br><br>Further, the Authority agreed to amend the section and incorporate the suggested verbiage. | **Section 3 D (15) amended to read as follows:**<br><br>"…If an **eligible** introducer or suitable certifier has met the customer, they must confirm to the FSP that they have met the customer via video-conferencing, including a photograph **of the customer** or scanned copy of the **certified** documents" |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | New Provision 15 refers to a ''suitable certifier'' and provides that such certifier must take photographs or scans of the relevant documents provided. This should be clarified / expanded to expressly confirm whether the relevant documents need to be certified. | The proposed amendments to the GNs seek to clarify the obligations of FSPs as it relates to the certification of identification documents and the obligations are already enshrined in **Section 4 B (30), (31) and (32)** of the Guidance Notes.<br><br>Photograph of the customer and scanned copies of the documents should be certified. | No amendment required. |
| | | Provision 15 references the use of video-conferencing when used by introducers or certifiers.<br><br>It would be useful if general guidance in respect of certification (using digital measures or paper proofs) could be deemed acceptable by FSPs on a risk based approach where there is not explicit confirmation of "true likeness".<br><br>General guidance outlines that a "copy should only be accepted where it has been certified by a suitable certifier as being a true copy of the original document and that the photo is a true likeness of the applicant." | The Authority is satisfied with the Section as is and no further amendment is needed in this regard.<br><br>For clarity, the Authority expects that where the eKYC/Digital ID technology is new, a formal risk assessment should be carried out. | No further amendment required. |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | Experiential knowledge has demonstrated that appropriately qualified certifiers do not always include the exact reference to "true likeness" however the certification meets all other requirements. Applying a risk based approach to these scenarios will ensure FSPs have the ability to accept copy documents without reverting to certifiers in some instances which may come at a cost to customers/related parties themselves.<br><br>**Suggested amendment:**<br><br>"A copy should only be accepted where it has been certified by a suitable certifier as being a true copy of the original document and that the photo is a true likeness of the applicant. However, an FSP may adopt a risk based approach to accept certified documents in the absence of true likeness being stated, provided the certifier themselves is deemed an appropriate and respectable certifier (by the FSP) and no doubts or higher risk characteristics exist or are identified in respect of the veracity of the document provided." | | |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | To further support this risk based approach, details of the certification regime for Guernsey by the Guernsey Financial Services Commission (GFSC) within the Handbook on Countering Financial Crime and Terrorist Financing have been provided below:<br><br>The obligations in respect of certification are as follows:<br>"the certifier should be a trusted third party who, in the case of natural person certification, has seen the original identification data and, where that identification data includes a photograph, met the individual in person. Only following these two steps can the certifier provide the necessary assurance to the firm about the individual's identity."<br><br>Further details are provided in the Handbook in respect of what is expected from the certifier and the standing of the certifier themselves, however there is no specific reference to a requirement for "true likeness" to be stated within the certification itself.<br><br>In addition to this, the Isle of Man Financial Services Authority (IOMFSA) Anti-Money Laundering | | |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | and Countering the Financing of Terrorism ("AML/CFT") Handbook also provides guidance on acceptable certification procedures which does clarify that the certifier should have met a customer to ensure photographic documents reflect a good likeness, it is not explicit that the certification need to confirm such wording.<br><br>"The certifier should also have met the individual face to face in order to ensure any photograph of the customer is a good likeness and the document corresponds to the person whose identity is being verified."<br><br>Aligned to FSPs providing their own risk based approaches to their procedures it is believed pragmatism can be applied in the circumstances described initially within this section of feedback, rather than an overly prescriptive and restrictive approach being deployed in every single scenario/instance. | | |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | Is video conferencing not considered face to face? What is an appropriate control and what is the risk the Authority is trying to address? Record date time etc? Can you provide examples of what is required?<br><br>For example - When using video conferencing the FSP should verify that who they are speaking to is who they purport to be by viewing identity documents, should true likeness be documented, etc.<br><br>This wording suggests that E-KYC is seen as lesser standard than certified documents which is not necessarily the case.<br><br>It appears to be questioning the judgment of the "suitable" certifier. What is the real risk of impersonation or stolen identity through the use of video conferencing that we are trying to mitigate? People feel more comfortable meeting people over video conferencing. | The risk that the Authority is trying to address is that the identifying documents may not be a true representation of the customer.Therefore, the Authority expects FSPs to seek alternative means to verify documents in situations where video-conferencing fails. Such as obtaining original certified true copies or soft copies digitally signed by a suitable certifier attesting to the authenticity of the documents. | No amendment required. |
| | | Paragraph 15 in the revised draft Guidance Notes contains a typo (needs a "met" in the second to last line). | Please see the response provided above. | No further amendment required. |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | Greater distinction needed between end-to-end digital ID systems - that conduct systems-based verification - and video conferencing as a means to replicate FTF contact remotely. Having these mixed in the same section may be misleading. Is a formal documented risk assessment (as per new Section 3D, 14) required to use e.g. Microsoft Teams, for verification of ID docs? Or is it adequate to implement appropriate processes and controls to mitigate risks such as poor connection/visibility?<br><br>Consequently, this paragraph could read better as a separate section, worded as follows:<br><br>"The use of video conferencing as a means to validate and verify the authenticity of ID documents must be applied in accordance with a risk-based approach. Appropriate processes and controls must be implemented to ensure that risks associated with this delivery channel are appropriately managed and mitigated".<br>Typo in footnote - "stimulates" should read 'simulates". | | |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| **13.** | **Part II – General AML/CFT Guidance**<br>**Section 3 D (16)**<br>"Customer identification and transactions that rely on reliable independent digital ID systems with appropriate risk mitigation measures in place which have been approved by a credible body may present a standard level of risk" | Industry can benefit from examples of a "credible body" that can approve a digital ID system. | The Authority agrees to amend **Section 3 D (16)** for clarity. | **Section 3 D (16) amended to read as follows:**<br><br>"Customer identification and ~~transactions~~ **verification** that rely on reliable **e-KYC**/independent digital ID systems with appropriate risk mitigation measures in place ~~which have been approved by a credible body~~ **that meet ISO/IEC technical global standards for digital ID systems** may present a standard level of risk, **and may even be lower-risk where higher assurance levels are implemented and/or appropriate ML/TF risk control measures, such as product functionality limits, are present**." |
| | | Approved by a credible body – greater definition is required here as to what is acceptable as this is vague at best. | The Authority agrees to amend **Section 3 D (16)** for clarity. | |
| | | Examples of credible bodies required. Reference to para 18 of FATF Guidance. "Where authorities do not audit or provide certification for IDSPs themselves, they are encouraged to support assurance testing and certification by appropriate expert bodies". The flow chart used throughout the FATF Guidance is predicates on authorities specifying the assurance levels of the digital ID system (e.g. pages 8 & 48 of the Guidance). | Please see Authority's response above. | |
| | | Who is the credible body? Government? Or independent party? This suggests digital ID system should have an assigned level of risk – this should be focused on customer risk not the system risk.<br>The assessment of system risk is included in the business risk assessment as part of technology and so has already been covered in the guidance notes.<br>Request to remove this comment. | Amended as recommended .<br><br>Please see Authority's response above. | |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | It is unclear both (a) who or what would be a 'credible body' in this context and (b) and what type of approval would be required to satisfy this requirement. If the Authority wishes to keep this wording, we would request that this is clarified. If this requirement cannot be clarified at this point in time, then it should not be imposed. Further, is the intention here that if the requirement for the system to be 'approved by a credible body' is not met, does this mean that the risk is by default a high risk? If so, we do not agree with this conclusion.<br>Our suggestion is that the following alternative wording is used:<br><br>**Suggested amendment:**<br><br>"Customer identification and transactions that rely on reliable independent digital ID systems with appropriate risk mitigation measures in place which have been adopted in accordance with this Guidance may present a standard level of risk."<br><br>Consider replacing the word 'transactions" with the word "verification". | | |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | Paragraph 16 of Section 3 D provides:<br>Customer identification and transactions that rely on reliable independent digital ID systems with appropriate risk mitigation measures in place which have been approved by a credible body may present a standard level of risk.<br>The FATF Guidance on Digital ID, 2020 ("FATF Guidance") states on page 11, paragraph 25:<br>"25 If, as a matter of internal policy or practice, non-face-to-face business relationships or transactions are always classified as high-risk, consider reviewing and revising those policies to take into account that customer identification/verification measures that rely on reliable, independent digital ID systems, with appropriate risk-mitigation measures in place, may be standard risk, and may even be lower risk. (Our emphasis)<br><br>The FATF Guidance goes onto state on page 30, paragraph 89:<br><br>"89. Given the evolution of digital ID technology, architecture, processes, and the emergence of consensus-based open-source digital ID technical standards, it is important to clarify that non-face- | Please see Authority's response above. | No further amendments required. |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | to-face customer-identification and transactions that rely on reliable, independent digital ID systems with appropriate risk mitigation measures in place, may present a standard level of risk, and may even be lower-risk where higher assurance levels are implemented and/or appropriate ML/TF risk control measures, such as product functionality limits and other measures discussed in INR10 and FATF Guidance on Financial Inclusion, are present..." (Our emphasis)<br><br>Given the FATF Guidance, we recommend that paragraph 16 of **Section 3D** be amended to specifically refer to 'verification', and to note the possibility for such digital ID systems to be 'lower-risk' where higher assurance levels and/or appropriate ML/TF risk controls are present.<br><br>**Suggested amendment:**<br><br>Customer identification/verification and transactions that rely on reliable independent digital ID systems with appropriate risk mitigation measures in place, which have been approved by a credible body, may present a standard level | | |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | of risk, and may even be lower-risk where higher assurance levels are implemented and/or appropriate ML/TF risk control measures, such as product functionality limits, are present." | | |
| **14.** | **Part II – General AML/CFT Guidance**<br>**Section 3 D (17)**<br>"FSPs shall adopt appropriate anti-fraud and cybersecurity measures to support digital ID/e-KYC technology, such as authentication systems for CDD purposes." | The authority should include additional information such as an example from the FATF (2020), Guidance on Digital Identity from paragraph 26, to guide the industry.<br><br>Proposed Wording:<br>" 17. FSPs shall adopt appropriate anti-fraud and cybersecurity measures to support digital ID/e-KYC technology, such as authentication systems for CDD purposes. For example, FSPs may utilise safeguards built into digital ID systems to prevent fraud to feed into systems to conduct ongoing due diligence on clients and to monitor, detect and report suspicious transactions." | The Authority has noted this comment and will include the suggested amendment in a footnote to provide examples of authentication systems for CDD purposes. | **New Footnote 15 added to read as follows:**<br><br>"For example, FSPs could utilise safeguards built into digital ID systems to: prevent fraud from feeding into systems; conduct ongoing due diligence on clients and business relationship; and monitor, detect and report suspicious transactions to relevant authorities" |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | FSPs should not be required to adopt new anti-fraud and cybersecurity measures where existing measures already provide appropriate protections.<br>In addition, authentication is part of the purpose of using digital ID/e-KYC systems. For example, an FSP will likely purchase third-party technology to authenticate documents digitally, for example, and that technology will have the authentication function built into the service/design. Accordingly, including this requirement does not make sense in this context.<br><br>Our suggestion is that this paragraph is re-phrased.<br>Suggested re-wording:<br>"FSPs shall ensure that their anti-fraud and cybersecurity measures accommodate and consider digital ID/e-KYC technology." | This provision does not stipulate additional anti-fraud and cybersecurity measures, rather it stipulates the "appropriate" measures.<br><br>For further guidance on Cybersecurity, FSPs may refer to the ***Statement of Guidance on Cybersecurity for Regulated Entities*** issued by the Authority, where applicable. | **Section 3 D (17) amended to read as follows:**<br><br>FSPs shall adopt appropriate anti-fraud and cybersecurity measures to support **e-KYC/**digital ID technology **systems**, such as authentication systems for CDD purposes. |
| | | Remove this is included in the assessment of the technology.<br><br>Consider replacing the word "technology" with the word "system".<br><br>Anti-fraud and cybersecurity are different concepts. CIMA should consider treating them as separate concerns. | The proposal to delete **section 3 D (17)** was not adopted since it is part of the risk assessment of technology and provides guidance pertaining to anti-fraud and cybersecurity measures. | No amendment required. |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | FSPs shall adopt appropriate anti-fraud and cybersecurity measures to support digital ID/e-KYC technology - these are matters to be considered by the vendor or supplier of the e KYC system, not the FSP.<br><br>What is being requested here? Surely these are matters for the vendor not the FSP, how would these be built in? | This provision does not stipulate additional anti-fraud and cybersecurity measures, rather it stipulates the "appropriate" measures an FSP should take to support digital ID/e-Kyc technology.<br><br>For further guidance on Cybersecurity, FSPs may refer to the ***Statement of Guidance on Cybersecurity for Regulated Entities*** issued by the Authority, where applicable. | No further amendment required. |
| **15.** | **Part II – General AML/CFT Guidance**<br>**Footnote 4**<br>"Remote onboarding is the establishment of new business relationships via technology and non-face-to-face means where the customer is not physically present at the place where the relationship is being established." | At **Footnote 4**, the phrase ''remote onboarding'' is defined to include non-face-to-face means where the customer is not physically present. Table 1 – Summary of AML/CFT Regulations on Remote On-boarding (at page 12) however states that video conferencing is a form of remote onboarding. Footnote 4 and/or Table 1 should be clarified to confirm whether: (i) the Authority deems video conferencing to be ''non-face-to-face''; or (ii) "non-face-to-face" simply means ''not physically present in person''. | By definition, video-conferencing "simulates" face-to-face meeting, which means it achieves the same outcome. The definition of remote onboarding describes technology (which includes face-to-face enabling video-conferencing) as well as non-face-to-face.<br><br>The Authority is of the view that there is no obscurity between e-KYC and remote onboarding. Definition of non-face-to face business relationships | No amendment required. |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | FATF has given video identification as an example of e-KYC. This Consultation Paper seems to distinguish e-KYC from remote onboarding. As such, the interplay between e-KYC and remote onboarding (as used in the proposed amendments, is unclear). | is already provided in the relevant section (e.g., ***Section 10)*** of the GNs. | |
| | | The definition of video-conferencing is useful, however, is it correct that the definition allows for video-conferencing to be considered as a true face-to-face measure? | Video-conferencing, is a simulation of a face-to-face meet, where a customer is not physically present. It is one example of verification among other e-KYC methods.<br><br>Guidance in relation to the use of video-conferencing is already provided in **Section 15** of the GNs. | No amendment required. |
| | | Footnote: in line 2, the word "stimulates" should be replaced with "simulates".<br><br>This makes clear that video-conferencing is acceptable to onboard customers who are legal persons and identify natural persons associated with legal persons, however, please can this be clarified whether this extends to using video-conferencing for verification purposes? | Please see the response provided above for **Footnote 14**. | No amendment required. |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| **16.** | **Part II – General AML/CFT Guidance**<br>**Footnote 5**<br>"… E-KYC refers to the processes whereby a customer's identity is verified via electronic means." | In footnote 5, the phrase ''e-KYC'' refers to the identification of a customer via electronic means. This should be clarified / expanded to expressly confirm whether e-KYC is intended to include identification of a customer by way of video conferencing. | Video-conferencing is one example of verification among other e-KYC methods.<br><br>Guidance in relation to the use of video conferencing is already provided in **Section 3 D of Part II** of the GNs. | No amendment required. |
| **17.** | **Part II – General AML/CFT Guidance**<br>**Footnote 6**<br>" [3]Video-conferencing is live, visual connection between two or more remote parties over the internet that stimulates a face-to-face meeting." | We consider 'stimulates' is a typo and should instead be 'simulates'.<br><br>Suggested re-wording:<br>"… Video-conferencing is a live, visual, and audio method of communication between two or more remote parties over the internet that simulates a face-to-face meeting." | The Authority notes and agrees with this recommendation. | **Footnote 14** amended to read as follows:<br><br>"Video-conferencing is live, visual connection between two or more remote parties over the internet that ~~stimulates~~ **simulates** a face-to-face meeting. **Video-conference is an e-KYC mechanism and is not considered face-to-face."** |
| | | The definition of video-conferencing is useful, however, is it correct that the definition allows for video-conferencing to be considered as a true face-to-face measure? | By definition, video-conferencing "simulates" face-to-face meeting, which means it achieves the same outcome. The definition of remote onboarding describes technology (which includes face-to-face enabling video-conferencing) as well as non-face-to-face means, | No further amendment required. |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | | therefore there is no conflict between the two definitions.<br><br>Definition of non-face-to face business relationships is already provided in the relevant section (e.g., **Section 10**) of the GNs. | |
| | | The definition should be reworded to account for instances:<br>1. where the subject is seen face to face by staff, but on a different day from the day in which the relationship is being established.<br>2. of Group Introduction as allowed for in Part VI Section 1 F 9 and 10. The majority of the Cayman Islands business is brought in through relationship managers based in other jurisdictions but working for the same organizations. These persons meet subject face to face, and the GN already allows for this type of treatment.<br><br>**Suggested amendment:**<br><br>Remote onboarding is the establishment of new business relationships via technology and non-face-to-face means where the customer is not physically present, or has not been present at any time before, at the place where the | Please see response provided above. | No further amendment required. |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | relationship is being established, or through a related (by way of common ownership) Financial Service Provider. | | |
| **18.** | **Part II – General AML/CFT Guidance**<br>**Footnote 12**<br>"A digital ID system is a system that covers the process of identity proofing/enrolment and authentication. Identity proofing and enrolment can be either digital or physical (documentary), or a combination, but binding, credentialing, authentication, and portability/federation must be digital.- FATF Guidance on Digital ID, 2020 E-KYC refers to the processes whereby a customer's identity is verified via electronic means." | The first sentence of **Footnote 12** is missing the words 'system is'. It currently reads:<br>A digital ID a system that covers the process of identity proofing/enrolment and authentication.<br><br>Suggested wording:<br>A digital ID system is a system that covers the process of identity proofing/enrolment and authentication.<br>Please note that this is only an issue in the Guidance Notes and not in the PSCP. | The proposed edit has already been addressed by the Authority. | No further amendment required. |
| | | This definition could be clarified as it suggests that the current method used by most service providers, whereby collecting a certified copy of a document that is then delivered electronically through email is E-KYC.<br>The intent of E-KYC encompasses the remote, paperless process. The definition should differentiate current practices (KYC) from digital verification (EKYC). KYC is currently achieved through offline (in person) and online (remotely) by delivery of certified documents. E KYC is | E-KYC (electronically know your client), comprises of all the processes a customer's identity is verified via electronic means such as email, video conferencing etc. And documents received via email can be accepted by an FSP provided that the FSP takes a RBA and has suitable documented policies and procedures in place to ensure authenticity of the electronic | No amendment required. |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | completely digital and verification can be achieved almost instantly by the chosen software.<br><br>Should there be a separate definition of E-ID compared to E-KYC? Does the definition include both in house and off the shelf tools? Lastly, does this also include a video conferencing whereby you verify the passport to someone's face? Definition should be expanded | documents. Additionally, E-ID are leveraged for e-KYC practices.<br><br>Video conferencing is an example of e-KYC processes. Section 3 D of these GNs provides more guidance on identity verification via video conferencing. | |
| **19.** | **Part II – General AML/CFT Guidance**<br>**Footnote 24**<br>Non-face to face business relationships – the establishment of business relationships and carrying out of transactions where the customer is not physically present at the place where the relationship is being established or transaction is conducted. | This Guidance is very specific about being physically present. Everything is on a case-to-case basis. We suggest including video conferencing in the face-to-face definition – observe through live video and consider sector specific guidance.<br><br>Is the transaction at a certain point in time.<br>Would the Authority consider a relationship non face to face if there has been an occasion to meet the customer over a period of time?<br><br>**Suggested amendment:**<br><br>Non-face-to-face business relationship at the establishment of a business relationship or the carrying out of a transaction where the customer is not physically | The Authority agrees to the proposed amendment. | **Footnote 16 revised to read as follows:**<br><br>Non-face-to-face business relationship at the establishment of a business relationship ~~of~~ **or** the carrying out of a transaction where the customer is not physically present at the place where the relationship is being established or transaction is conducted. |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | present at the place where the relationship is being established or transaction is conducted. | | |
| **20.** | **Part II – General AML/CFT Guidance**<br>**Section 3 D 18 (3) but should be corrected to (2)**<br>When assigning high risk ratings relating to products, services and delivery channels, FSPs should consider:<br>(1) the level of transparency, or otherwise of the product, service or transaction (e.g. the extent to which the products or services facilitate or allow anonymity or opaqueness of the customer, ownership or beneficiary structures that could be used for illicit purposes);<br>(2) non-face-to-face business relationships and/or occasional transactions when other high-risk factors have been identified. | Is it the expectation of the regulator that the licensee will define scenarios whereby the licensee will not conduct non-face-to-face business relationships? For example, if the licensee principally operates an online business, it may be difficult for that particular licensee to only implement face-to-face onboarding processes. | Yes, the Authority expects FSPs to define scenarios where they do not conduct face-to-face business relationships.Since,non-face -to -face business relations and transactions present circumstances where the risks of ML or TF may potentially be higher. | No amendment required. |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| **21.** | **Part II – General AML/CFT Guidance**<br>**Section 3 D (19)**<br>"In assigning lower risk classifications relating to products, services and delivery channels, FSPs may consider:<br><br>(1) financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes;<br>(2) products and services that do not encourage early surrender options (e.g. in the case of insurance policies for pension schemes);<br>(3) products that cannot be used as collateral; and<br>(4) products that with strict rules that do not permit the assignment of a member's interest (e.g., a pension, superannuation or similar scheme, where contributions are made by way of deduction from wages)." | Paragraph 19 of Section 3 D sets out 'Low-risk Classification Factors' for products, services and delivery channels. We note that there are currently no Low-risk Classification Factors listed for delivery channels. While we appreciate that there are risks associated with digital ID systems, there are also risks associated with traditional documentary ID systems. As the FATF Guidance states at paragraph 113, on page 39:<br><br>"In both documentary and digital ID systems, for example, reliability can be undermined by identity theft and source documents that can be easily forged or tampered with. Some types of fraud may be less likely to occur in-person or in processes requiring human intervention, including 'massive attack frauds' which are more likely to happen remotely. While digital ID systems provide security features – e.g., secure authentication – that mitigates some issues with paper-based systems, they also increase some risks, such as data loss, data corruption or misuse of data due to unauthorised access."<br><br>While paragraph 20 of Section 3 D indicates that the examples of risk | The Authority notes that this comment falls outside the scope of this consultation and will be considered and addressed in due course. . | No amendment required. |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | factors/indicators are not intended to be comprehensive, we suggest that paragraph 19 be amended to include an example of a Low-risk. Classification Factor for digital ID systems. This would enable Financial Service Providers to have confidence that in certain circumstances, for example, where a particular digital ID system has been approved by a credible body as having the highest possible levels of assurance (confidence), that it could assign a lower risk classification to that delivery channel. This is especially important considering that this is an evolving area, and the FATF Guidance indicates that with appropriate risk mitigation measures in place, digital ID systems 'may even be lower-risk."<br><br>Suggested wording:<br>"19. In assigning lower risk classifications relating to products, services and delivery channels, FSPs may consider:<br>…<br>(3) products that cannot be used as collateral;<br>(4) products with strict rules that do not permit the | | |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | assignment of a member's interest (e.g., a pension, superannuation or similar scheme, where contributions are made by way of deduction from wages); and<br><br>(5) digital ID systems which have been approved by a credible body as having the highest levels of assurance." | | |
| **22.** | **Section 3 E 2 (g)**<br>Procedures for the regular, ongoing and independent review of the effectiveness of systems and processes used. | Clarity on whether a footnote should be added to clarify that an independent review does not necessary mean by an external body, and can be conducted by the internal audit function or 'third line of defense" | The Authority added a new footnote that speaks to the onus of independent reviews. | **New footnote 18, added and reads as follows;**<br><br>Independent review may be conducted by internal audit or any other control function as defined within Rule: Corporate Governance for Regulated Entities. |
| **23.** | **Part II – General AML/CFT Guidance**<br>**Section 3 G (2) (g)**<br>"FSPs should have robust documented policies and procedures in place to ensure a consistent and adequate approach to relying on existing or new digital ID system/technology solutions for CDD purposes. These may include (but are not limited to):<br>a. A tiered CDD approach that leverages technology | This section lacks clarity on who would perform an independent review and the standard of the effectiveness required. If an FSP purchases a third-party technology solution, it will be extremely difficult for an FSP to arrange an independent review. Such review or quality certification will likely be built into the service provider's own requirements to enable FSPs to use and rely on their product, which would be taken into account as part | The Authority expects an FSP to conduct digital ID system/technology solutions audits on a regular basis. The frequency of the audit should be commensurate with the FSP's nature, size, complexity and risks identified during the risk assessments.<br>Where an FSPs, uses and relies on third party | No amendment required. |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | solutions with various assurance levels;<br>b. Policies for the secure electronic collection and retention of records;<br>c. A process for enabling authorities to obtain the underlying identity information and evidence needed for identification and verification of individuals;<br>d. Anti-fraud and cybersecurity processes to support e-KYC/digital ID proofing and/or authentication for AML/CFT efforts;<br>e. Back-up plans for possible instances where the technology solution fails; | of the risk assessment of any new technology to be used. If the Authority wishes to keep this wording, we would request that this is clarified.<br><br>Our suggestion is that this paragraph is re-phrased.<br><br>**Suggested amendment:**<br><br>"Procedures for the regular and ongoing assessment or review of the systems and processes used." | product, the ultimate responsibility for CDD measures remains with the FSP.<br><br>Additionally, FSPs should maintain policies and procedures in relation to outsourcing where they intend to outsource some of their functions, as provided for in **Section 10 C** of the GNs.<br><br>For further guidance on outsourcing, FSPs may refer to the ***Statement of Guidance on Outsourcing*** issued by the Authority, where applicable. | |
| | f. A description of risk indicators that would prompt a FSP to refrain from utilising digital ID system/technology solutions; and<br>g. Procedures for the regular, ongoing and independent review of the effectiveness of systems and processes used." | Section 3 G (2)(g) sets out certain policies and procedures that could be included in a Financial Service Provider's documented policies and procedures for relying on existing or new digital ID systems/technology solutions for CDD purposes.<br><br>We recommend that the Guidance Notes be clarified to confirm that such review could be undertaken either internally (i.e., via the internal audit function), or externally. | Please see the response provided above. | No further amendment required. |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | Suggested wording:<br>*g*. Procedures for the regular, ongoing, and independent review (whether internal or external) of the effectiveness of systems and processes used." | | |
| | | On the licensees use of technological service providers, will the revised guidance cross-refer to the Authority's statement of guidance on outsourcing? | Yes. For further guidance on outsourcing, FSPs may refer to the **Statement of Guidance on Outsourcing** issued by the Authority, where applicable. | No amendment required. |
| | | These inclusions do not add value on top of what is already included in Section 3G, and the Rules and SOG on Cybersecurity for Regulated Entities. Inserting this entire section adds volume with no increase in value.<br><br>Delete section and make reference to the Rules and SOG on Cybersecurity for Regulated Entities**.** | The Authority is of the opinion that this section provides necessary and sufficient guidance on the use of new digital ID systems/ technologies. | No amendment required. |
| | | This paragraph 2 is located under the heading "G. NEW PRODUCTS AND TECHNOLOGIES".<br>Therefore, in line 2, the deletion of the words "existing or" should be considered. The addition of the words in red, above, should also be considered. | The Authority agrees to the proposed amendment. | **Section 3 G (2), revised to read as follows;**<br><br>2. FSPs should have robust documented policies and procedures in place to ensure a consistent and adequate |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | a) Various risk levels not various assurance levels. b) Covered in other sections of the guidance notes – make sure policy consider documented policies and procedures contain the following.<br><br>**Suggested amendment:**<br><br>1. FSPs should have robust documented policies and procedures in place to ensure a consistent and adequate approach to relying on existing or new digital ID system/technology solutions for CDD purposes. These may include (but are not limited to):<br>a. A tiered CDD approach that leverages new technology solutions with various assurance levels;<br>b. Policies for the secure electronic collection and retention of records created by new technology solutions;<br>c. A process for enabling authorities to obtain from the new technology solutions the underlying identity information and evidence needed for identification and | | approach to relying on ~~existing or~~ new digital ID system/technology solutions for CDD purposes. These may include (but are not limited to):<br>a) A tiered CDD approach that leverages **the new** technology solutions with various assurance levels;<br>b) Policies for the secure electronic collection and retention of records **by the new technology solutions**;<br>c) A process for enabling authorities to obtain **from the new technology solutions** the underlying identity information and evidence needed for identification and verification of individuals;<br>d) Anti-fraud and cybersecurity |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | verification of individuals;<br>d. Anti-fraud and cybersecurity processes to support e-KYC/digital ID proofing and/or authentication for AML/CFT efforts resulting from the new technology solutions;<br>e. Back-up plans for possible instances where the new technology solutions fail;<br>f. A description of risk indicators that would prompt a FSP to utilising new digital ID system/technology solutions; and<br>g. Procedures for the regular, ongoing, and independent review of the effectiveness of the new systems and processes used. | | processes to support e-KYC/digital ID proofing and/or authentication for AML/CFT efforts **resulting from the new technology solutions;**<br>e) Back-up plans for possible instances where the **new** technology solutions fail;<br>f) A description of risk indicators that would prompt a FSP to utilising **new** digital ID system/technology solutions; and<br>**g)** Procedures for the regular, ongoing, and independent review of the effectiveness of the **new systems** and processes used.<br>. |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| **24.** | **Part II – General AML/CFT Guidance**<br>**Section 4 A (16) (1) (d)**<br>As two aspects of one process, these requirements are likely to interact and complement each other naturally. In this context, FSPs should:<br>(1).Identify the applicant and verify its identity. The type of information that would normally be needed to perform this function would be:<br>(a) Name, legal form and proof of existence – verification could be obtained, for example, through a certificate of incorporation, a certificate of good standing, a partnership agreement, a deed of trust, or other documentation from a reliable independent source proving the name, form and current | This inclusion is unnecessary since video conferencing is referred to earlier.<br><br>Delete addition. | The Authority has determined Video-conferencing as a requirement for CDD is necessary for FSP and therefore the Authority will retain the section. | No amendment required. |
| | | Is it also possible to use publicly available information of the regulatory authority for verification purposes?<br><br>Provision 16 (1) (d) makes clear that regulated entities may use publicly available sources, including company registries as sources of verification for legal persons.<br><br>Where firms are currently progressing remedial activities in respect of existing customer relationships, (which are likely to continue and overlap with the progression and deployment of the changes highlighted in the consultation), is it acceptable for firms to commence using public | The Authority expects FSPs to undertake reasonable search of public information including company registries for verification purposes.<br><br>For Further guidance on identification information and verification procedures, FSPs should refer to **Section 4 (B**) of the Guidance Notes. | No further amendment required. |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | existence of the customer.<br>(b) The constitutional documents that regulate and bind the legal person or arrangement (e.g. the memorandum and articles of association of a company), as well as the names of the relevant persons holding a senior management position in the legal person or arrangement (e.g. directors, senior managing directors in a company, trustee(s) of a trust).<br>(c) The address of the registered office, and, if different, a principal place of business.<br>(d) When verifying customers that are legal persons, regulated entities may use publicly available sources, including company registries**.** | registries (where deemed appropriate) for verification immediately?<br><br>This will help to ensure customer remediation is aligned to the planned industry guidance ahead of full deployment of the regulatory changes and consistency will therefore be applied to the customer base rather than seeking copy<br>documents from some customers that have been prioritised for remediation ahead of those to be remediated at a later date. | | |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| **25.** | **Part II – General AML/CFT Guidance**<br>**Section 4 A (17)**<br>The use of video-conferencing to onboard customers who are legal persons or arrangements may be used to identify natural persons such as ultimate beneficial owners, settlors, trustees, protectors, or those appointed to act on behalf of the customer. | We consider that 'directors and officers' should be added to this list.<br><br>Suggested re-wording:<br>"The use of video-conferencing to onboard customers who are legal persons or arrangements may be used to identify natural persons such as directors, officers, ultimate beneficial owners, settlors, trustees, protectors, or those appointed to act on behalf of the customer." | The Authority notes and agrees with this recommendation.<br><br>The list of natural persons is not exhaustive. | **Section 4 A (17) amended to read as follows:**<br><br>The use of video-conferencing to onboard customers who are legal persons or arrangements may be used to identify natural persons such as **directors, officers,** ultimate beneficial owners, settlors, trustees, protectors, or those appointed to act on behalf of the customer. |
| | | Is this "may be used to identify" or "may be used to validate and verify the authenticity of ID documents" - see amendments above. | The Authority believes the Section is properly construed as is. | No amendment required. |
| | | Provision 17 makes clear that video-conferencing is acceptable to onboard customers who are legal persons and identify natural persons associated with legal persons, however, please can this be clarified whether this extends to using video-conferencing for verification purposes? | The Authority expects FSPs usage of video-conferencing to be in accordance with a risk-based approach.<br><br>Additionally, FSPs should put in place appropriate controls during video conferencing process to verify the identity and authenticity of the ID documents. | No further amendment required. |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| **26.** | **Part II – General AML/CFT Guidance**<br>**Section 4 A (18)**<br><br>FSPs who are unable to verify official documents such as certificates of incorporation and trust deeds presented during video-conferencing or via other electronic methods due to unavailability of public sources must seek alternative measures to verify the documentation. This may include obtaining an original certified true copy or accepting soft copies digitally signed by a suitable certifier attesting to the authenticity of the documents. | This inclusion is unnecessary. The GN and Regs say you must identify and verify. So if the tool fails in that regards, then the subject has not been verified and you must comply with Section 4B 37.<br><br>Delete addition.<br><br>**Suggested amendment:**<br><br>Include wording of "verifications though other means" and remove last sentence. A certifier is not qualified to attest to the authenticity of documents (e.g forged or altered), they attest to a true copy of the document produced before them. | The proposed amendments to the GNs seek to clarify the obligations of FSPs as it relates to the certification of identification documents.<br><br>Additionally, **Section 4 B (30),(31) and (32)** of the Guidance Notes provides further guidance re certifiers. | No amendment required. |
| | | Clarify how video conferencing would work to identify and verify statutory documents - is this vis a vis entry in a government registry? Is additional verification required where an entity is listed a government registry or is the new 4C, 16, 1(d) sufficient? FATF Guidance on Digital Identify does not contemplate using video conferencing in this manner | The provision speaks to being unable to conduct subsequent verification of documents that were "presented" during a video-conference call or via other electronic means. The applicant for business may present certificate of incorporation as part of the onboarding process, but the onus is on the FSP to verify the information provided.<br>I.e., refer to a company registry to see if the | No amendment required. |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | | company does exist and has the particulars as outlined in the document (company registration number, date of incorporation, corporate purpose, list of directors etc.) Additionally, whilst the provision speaks to verification of documents, the FSPs may use document authentication tools to validate the legitimacy of a document. Guidance in relation to identification and verification is already provided for in **Part II Section 4B** of the GNs. | |
| **27.** | **Part II – General AML/CFT Guidance**<br>**Section 4 B (10)**<br>FSPs should have policies and procedures in place to address any specific risks associated with non-face to face business relationships and transactions**.** | Should there not merely be a modification to the section 35 below?<br><br>**Suggested amendment:**<br><br>Amalgamate new addition with non-face to face definition in 35. | The Authority agrees to the proposed amendment. | **Section 4 B (10)** and **4 B (35)** merged to circumvent replication |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| **28.** | **Part II – General AML/CFT Guidance**<br>**Section 4 B (20) and (21)**<br><br>Certification of documents through "selfie" documents, photographs or videos: Photographs should clearly show the person's face and the image on the identity document being held in the same picture to demonstrate this actually belongs to the customer. A clear scanned copy or photograph of the document itself should also be provided. | CIMA to clarify if this refers to digital ID systems or non digital ID processes/ eKYC.<br><br>If the process includes digital ID systems , then it should not be considered mandatory to have the selfie include the passport. Most digital ID systems use NFC and MRZ code scanning to authenticate the passport and "liveness" testing in the selfie, which is more reliable and could not be achieved if the passport was to be included. | **Section 4 B (20),** refers to e-KYC measures outside of digital ID systems, as opposed to ID systems which test the authenticity of ID documents. | No amendment required. |
| | | clarification needed on this existing guidance in the context of amendments and references to end-to-end digital ID systems. | Please see response provided above. | No further amendment required. |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | The Authority does not state, if the image is required to be in color? This assumes black and white photos are acceptable? We suggest clarification if this is not an accurate assumption.<br>Verification of documents through digital technology should not be equated to a "certification" process. The title of this section should be amended to read: "Standard of 'selfie' documents, photographs or videos."<br>Consider including the word "identity" after the words "photograph of the". | The Authority agrees to the proposed amendment. | **Section 4 B (20) amended to read as follows:**<br><br>~~Certification~~ **Verification** of documents through "selfie" documents, photographs or videos: Photographs should **be in colour and** clearly show the person's face, **holding** the **identity** document in the same **photograph** to demonstrate **it** actually belongs to the customer. A clear scanned copy **in colour** or photograph of the **identity** document itself should also be provided. |
| **29.** | **Part II – General AML/CFT Guidance**<br>**Section 4 C (1) and (2)**<br>Examples of the types of circumstances (in addition to those referred to above for beneficiaries of long-term insurance policies) where it would be permissible for verification to be completed after the establishment of the business relationship, because it would be essential not to interrupt the normal conduct of business, include: | The risk based approach has already been referenced as a precursor.<br><br>Delete addition. | Any interaction between an FSP and an applicant/customer in a non-direct manner increases the exposure to risk. By adhering to a RBA, FSPs should put into place policies and procedures that appropriately address such risks. | No amendment required. |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | (1) Non-face-to-face business, in accordance with a risk-based approach**.** | | | |
| **30.** | **Part II – General AML/CFT Guidance**<br>**Section 4 C (35)**<br><br>"Any interaction between an FSP and an applicant/customer in a non-direct manner increases the exposure to risk. Not only does this allow for third parties to have access to assets or property through impersonation but may also disguise the true owner of that property by, for example, provision of false identification documentation. FSPs should put into place policies and procedures that appropriately address the risks posed by non-face-to-face contact for customers at the opening of the business relationship and through the operation of that relationship. " | We consider 'through' is a typo and should instead be 'throughout'.<br><br>**Suggested amendment:**<br><br>"Any interaction between an FSP and an applicant/customer in a non-direct manner increases the exposure to risk. Not only does this allow for third parties to have access to assets or property through impersonation but may also disguise the true owner of that property by, for example, provision of false identification documentation. FSPs should put into place<br>policies and procedures that appropriately address the risks posed by non-face-to-face contact for customers at the opening of the business relationship and throughout the operation of that relationship." | The Authority notes and agrees to the proposed amendment. | **Section 4 C (35), amended to read as follows:**<br><br>Any interaction between an FSP and an applicant/customer in a non-direct manner increases the exposure to risk. Not only does this allow for third parties to have access to assets or property through impersonation but may also disguise the true owner of that property by, for example, provision of false identification documentation. FSPs should put into place policies and procedures that appropriately address the risks posed by non-face-to-face contact for customers at the opening of the business relationship and ~~through~~ **throughout** the operation of that relationship. |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| **31.** | **Part II – General AML/CFT Guidance**<br>**Section 5A (6)**<br><br>"FSPs may consider digital ID systems/e-KYC processes with lower levels of assurance to be sufficient for simplified due diligence in cases of low ML/TF risk." | This statement was taken from the FATF (2020), Guidance on Digital Identity but is incomplete and potentially mislead and does not address the original concept of adopting a risk-based approach.<br><br>See the original recommendation from FATF (2020), Guidance on Digital Identity below.<br>"24. Consider whether digital ID systems with lower assurance levels may be sufficient for simplified due diligence in cases of low ML/TF risk. For example, where permitted, adopting a tiered CDD approach that leverages digital ID systems with various assurance levels to support financial inclusion." | **Part II Section 5A (6)** speaks to the risk-based approach that the FSP should take in determining assurance levels of digital ID systems according to the levels of ML/TF risk exposure. General guidance in relation to simplified due diligence matters is provided in **Part II Section 5** of the GNs.<br><br>The Authority is satisfied that the proposed amendment provided is sufficient. | No amendment required. |
| | | Please consider 'no certification' in line with risk-based approach for lower risks clients.<br><br>Amendments stated that digital ID/E-KYC processes with lower level of assurance to be sufficient for simplified due diligence cases-does this confirm that if the system has no approval by a credible body (lower levels of assurance) that FSP's can still accept using this e-KYC method for low ML/TF risk cases which simplified due diligence can be applied? | The intention of the Authority is not to promote low assurance ID systems but to allow FSPs to utilize digital ID systems in accordance with a risk-based approach. The FATF guidance refers to a tiered CDD approach that leverages digital ID systems with various assurance levels to support financial inclusion.<br><br>For instance, to give access to excluded or underserved | No further amendment required. |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| | | Further, regardless of the assurance level, FSP will determine if the technology is suitable for their purposes. Already covered in the business risk assessment on technology. Suffice to say they would not use the system if it was not reliable, regardless of assurance level. Consider removing this clause. | individuals, some FSPs delay verification of the customer's identity until specified thresholds are reached or limitations are placed on the value and number of transactions within a specified timeframe.<br><br>Allowing low assurance systems for low-risk scenarios means that a formerly excluded person who lacks certain documents to provide proof of official identity can still be onboarded in a digital ID system. | |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| **32.** | **Part II – General AML/CFT Guidance**<br>**Section 8 A (3)**<br>FSPs must also ensure that records of identification data obtained through digital ID systems and e-KYC procedures are easily accessible, maintained and can be made available to competent authorities upon request. | What is the expectation from the Authority on retention / documentation of video conference calls?<br><br>Some key considerations outlined as an example but not limited to would assist Licensees. For example:<br>Is the licensee expected to record the video call? Should the licensee document:<br>> time and date> email address? | The FATF Guidance states that regulated entities should ensure that they have access to, or have a process for enabling authorities to obtain, the underlying identity information and evidence or digital information needed for identification and verification of individuals. It does not prescribe how this should be done. Digital records specifying the types of identity evidence used for specific evidence, including data source, date/time and means of accessing it may support this requirement.<br><br>For further guidance, FSPs may refer to the ***Statement of Guidance on Nature, Accessibility and Retention of Records*** issued by the Authority, where applicable. | No amendment required. |

| No. | Section | Comments | Authority's Response | Consequent Amendments to the Proposed Measure |
|---|---|---|---|---|
| **33.** | **Part V - Sector Specific Guidance: Insurance Sector Section 1 H (7) (1)**<br>It is recommended that EDD be applied for high risk situations and in situations where the insurer is particularly exposed to reputational risk. There will be certain occasions where EDD will be required, for example:<br>(1) when there is an identified high-risk factor accompanied by no face-to-face contact with the insurer;<br>(2) where the customer is a PEP;<br>(3) where the beneficiary of a policy can be transferred; and<br>(4) when the customer is involved in a business that is considered to present a high risk for ML/TF. | Update insurer to insured. | The Authority agrees to the proposed amendment. | **Section 1 H 7 (1) amended to read as follows:**<br><br>It is recommended that EDD be applied for high risk situations and in situations where the insurer is particularly exposed to reputational risk. There will be certain occasions where EDD will be required, for example:<br>(1) when there is an identified high-risk factor accompanied by no face-to-face contact with the ~~insurer~~ **insured**;<br>(2) where the customer is a PEP;<br>(3) where the beneficiary of a policy can be transferred; and<br>(4) when the customer is involved in a business that is considered to present a high risk for ML/TF. |