FSB & PB Handbooks on Countering Financial Crime and Terrorist Finance

Website FAQs

Q: What Bearing Does the Duration of a Business Relationship Have on Assessing the Risk Posed by a Customer?

A: On 30 June 2017 rule 56 of the Handbook for Financial Services Businesses on Countering Financial Crime and Terrorist Financing and rule 69 of the Handbook for Lawyers, Accountants and Estate Agents on Countering Financial Crime and Terrorist Financing were updated to include consideration of the expected duration of a business relationship.

With regard to the latter, for a large number of the products and services offered by firms the expected duration of a business relationship should be self-explanatory and likely understood at the commencement of a relationship due to the intrinsic nature of those products and services. Some products and services may have a shorter or more defined expected duration such as investments in a closed-ended fund, fixed term contracts for investments, loans and deposits, or the establishment of a pension. Conversely there may be some products and services such as current accounts, wealth management or fiduciary arrangements which may have no set duration and which could continue indefinitely, e.g. until the customer decides to close them or the customer ceases to be.

The duration of a business relationship should therefore not be considered as a variable in isolation when determining the overall risk rating of a customer. In this respect, a product or service with a long or indefinite lifespan, e.g. a current account with a bank or an investment in an open-ended collective investment scheme, would not be considered high risk because it has indefinite life; in the same way a short term product, e.g. a three month fixed deposit, would not be considered low risk because it has a limited "shelf life".

However, consideration should be given, both at the commencement of a business relationship and during subsequent periodic risk reviews, to the anticipated duration of the business relationship based on the nature of the product or service and whether this aligns with the reality of the relationship. In this respect a firm should ask itself if the rationale for continuing the relationship remains appropriate given the type of product or service provided and the use or otherwise made of it by the customer during the period under review.

Examples of potential higher risk factors in this regard could include:

- An investment in an open-ended collective investment scheme which is redeemed after an unexpectedly short space of time;
- A short-term fixed deposit account which has remained untouched for a much longer length of time than expected;
- The repayment of a loan in an unexpectedly short period of time following it being taken out;
- The cancelation of an insurance policy in an unexpectedly short period of time following it being taken out; or
- The unusual early cancellation of any other financial product or service that results in an economic cost to the customer.

For some products and services where there is no intrinsic duration, firms may consider utilising standardised assessments of duration, with specific consideration of this variable only where a customer deals outside of the expected norms for that product. An example would be an open-ended collective investment scheme where there is no defined duration for an investment. In this example the firm may have an understanding of the anticipated or standard duration of an investment in the scheme based upon the type of assets the scheme holds and the scheme's investment horizon/objective.

For existing customers, firms should give consideration to this additional risk factor when undertaking periodic risk reviews in line with firms' existing review cycles.

Q: Rule 30 - What Type of Events Should be Notified to the Commission?

A: Rule 30 of the FSB Handbook and Rule 46 of the PB Handbook require that the Commission be advised of any material failure to comply with the AML/CFT Regulations, rules in the Handbooks and any serious breaches of the policies, procedures and controls of the business ("Notification Rules").

The following are examples of the types of scenarios in which the Commission would expect to be notified under the Notification Rules:

- The business receives a report from an auditor identifying areas of non-compliance where remediation work is recommended.
- The business receives a report, whether orally or in writing, from an external party engaged to review its compliance arrangements, identifying areas of non-compliance where remediation work is recommended.
- The business is aware that the non-compliance may have occurred across more than one member of a corporate group of which it is a member.
- The business discovers that the party to whom it has outsourced certain compliance functions has failed to apply the AML/CFT Regulations and/or rules in the Handbook and remediation work is required.
- The non-compliance involves any country listed in the Commission's Instructions on Business from Sensitive Sources or sanction requirements, regardless of the number of business relationships/ occasional transactions involved.

Delay in Notification

The Commission considers the following reasons to constitute poor practice in relation to the corporate governance of a business for delaying notification under the Notification Rules:

- An auditor/ external reviewer has identified a number of areas of non-compliance but assessed these as low risk or low priority.
- The business lacks the resources to immediately address the non-compliance or seeks to undertake the necessary remediation work before notifying the Commission.
- Advice is received from a consultant that the non-compliance it has reported on is not considered "material" or "serious".
- There is no evidence that an actual financial crime has occurred as a result of the non-compliance.

Incidental Matters

The Commission recognises that from time to time a business may identify instances of non-compliance as part of its ongoing monitoring or customer risk review programs. Provided that these are isolated instances which are:

- readily resolvable within a short period of time, and
- do not compromise the accuracy of the business' understanding of the purpose and intended transaction activity of that relationship,

Such instances need not be reported to the Commission.

The Commission may still and reserves it right to enquire about such instances of non-compliance during on-site visits and thematic reviews.

Q: What is a Business Risk Assessment?

Introduction

Regulation 3 of the AML/CFT Regulations requires a business to carry out and document a suitable and sufficient business risk assessment ("BRA").

A BRA is an important tool used to identify, assess and decide how a business will mitigate its risk exposure to the particular types of financial crime risks to which it could be exposed.

Other benefits gained from performing a BRA are listed in Chapter 3 of the AML/CFT Handbooks.

The term "financial crime" is used in this guidance to describe money laundering, terrorist financing, corruption and bribery, and such other predicate offences as are listed in Chapter 1 of the Handbooks.

Identification of Financial Crime Risks

The first step to undertaking a BRA is in determining the potential financial crime risks to which the business could be exposed.

In order to be considered "suitable", the BRA must document consideration of the financial crime risks that are specific to its own business activities. The contents of the BRA should reflect an informed consideration of these risks.

A BRA will not be considered "sufficient" where it identifies generic risks such as "there is a risk that our products could be used to finance terrorism" or "the proceeds we receive may have been derived from bribery and corruption". A BRA will also not be considered suitable where it appears to list all possible forms of financial crime risks, regardless of their relevance or likelihood of occurrence, to the business.

A business must ask itself 'what is the threat of our business being used for financial crime?' For example, what risk is posed by the target/actual customer base, taking into account:

- The proportion which comprises of high net worth individuals and politically exposed persons,
- The geographic origin of customers, and where applicable, their controllers and beneficial owners,
- The proportion which will comprise of ongoing non face-to-face relationships, where reliance will be placed on third parties to verify customer identity (i.e. certifiers, introducers); and
- The complexity of customer structures and legal arrangements.

Sources of Information

There are a number of different sources of information about the financial crime risks relating to particular types of business activities, products, services, customers, transactions, delivery channels etc. Examples of some useful sources are listed at the end of this guidance.

Industry sectors will have inherent and/or generic risk factors and these will need to be referenced. Additionally, individual entities will also have risk factors particular to that entity which will need to be referenced in their BRA.

A BRA should not contain unsubstantiated, highly generalised references to risk faced by the business. For example, a reference to all business being low risk would not be acceptable unless it was backed up with sufficient information as to how this assessment had been made.

Consider Risk "In the Round"

Before moving to the next step, a business should step back and consider its "risk in the round". A business should not only consider each of the financial crime risks individually, but also whether their concurrent or confluent effect on one another, might raise its overall risk exposure.

Other operational factors may increase the overall level of risk. These include but are not limited to:

- The outsourcing of financial crime controls or other regulatory requirements to an external third party or a member of the group of companies to which the business belongs; or
- The use of on-line or web-based services and cybercrime risks which may be associated with those service offerings.

Assess & Mitigate the Financial Crime Risks

Having identified the financial crime risks, the business must then assess those risks and consider how they will be mitigated by the business. These measures may, for example, include:

- Varying CDD procedures appropriate to the assessed financial crime risks for certain customers,
- Requiring the quality of verification evidence – documentary/electronic/third party – to be of a certain standard,
- Allocating additional resources to allow for enhanced monitoring measures to be applied,
- Applying oversight measures and reporting requirements to third parties to whom compliance functions have been outsourced,
- Requiring review by the compliance function and approval by senior management to the take-on of new relationships; or
- Limit the acceptance of certain high risk business to a particular threshold, relative to the overall customer base of the business.

Each measure should be designed to address the identified risks. While a short summary of the specific measure to be applied may be suitable, it will not be sufficient for a business to record a generalised statement such as, "the business has policies and procedures in place to mitigate this risk".

Responsibility for the Assessment

The Board and senior management of any business are responsible for managing the business effectively. They are in the best position to evaluate all potential risks including financial crime risks.

The rules in chapter 2 of the Handbooks in relation to corporate governance make it clear that the Board has effective responsibility for compliance with the Regulations and the Handbook and therefore it must take ownership of and responsibility for the preparation and review of the BRA.

Businesses should also be alive to the Commission's FAQ on reliance on third parties, particularly where a third party is asked to prepare the BRA, which can also be found on this webpage.

Format of the Assessment

The format of an assessment is a matter to be decided by the business. Of critical importance is that the BRA is documented and records the assessment undertaken. The date on the assessment should be the day on which the BRA was reviewed and approved by the Board.

Tracked versions of a BRA should not be submitted when requested by the Commission as part of a pre-onsite visit unless it has been reviewed and approved by the Board, or equivalent, of the business.

Businesses are strongly discouraged from copying the assessment prepared by another business, or using an "off the shelf" assessment which pre-identifies suggested financial crime risks. It has been observed that businesses who do so frequently fail to accurately identify the financial crime risks specific to their business and adopt policies, procedures and controls that are either ill-suited or fail to mitigate their financial crime risks.

What should the BRA not contain?

- The BRA should not simply be a cut and paste version of the relevant sections of the Handbook.
- The BRA should not be a generic document which has simply been populated with general information.
- It should not be a mix of ML/FT and prudential risk. If the business wishes to combine the assessment of ML/FT and prudential risk in one document there needs to be a clear division between the two assessments.

Establishing Risk Appetite

Undertaking a business risk assessment allows the business to formulate its "risk appetite". The term "risk appetite" refers to a business' overall willingness or acceptance threshold for new business and the associated financial crime risks that will need to be mitigated.

A business should be able to formulate a statement, which is understood by all of its staff, about the limits of that appetite, beyond which it is not prepared to accept or able to effectively mitigate, the associated financial crime risks.

Review of the BRA

Regulation 3 of the AML/CFT Regulations requires that a business regularly review its BRA. This review must be undertaken at least annually, so as to keep it up to date. Where, as a result of that review, changes to the BRA are required, the business must make those changes.

Just as the activities of a business can change, so too do the corresponding financial crime risks. Mergers, acquisitions, the purchase or sale of a book of business, restructuring or a change of external service provider are just some of the events which can affect both the type and extent of financial crime risks to which a business is exposed. This can then result in a need for changes to be made to existing controls to mitigate those risks effectively.

Other operational changes such as a change in staffing numbers, change in technology or a change to group financial crime policies, can all have an impact upon the resources required to effectively mitigate financial crime risks.

Best practice indicates that a review of a BRA should occur whenever changes such as those described above occur and at least on an annual basis. This ensures that the policies, procedures and controls put in place to mitigate the financial crime risks specific to the business are and remain appropriate and effective.

Best practice also suggests that the business should maintain a log or record with its BRA recording the dates on which the BRA has been reviewed and, where necessary changed, and approved by the Board, or equivalent.

Self-Assessment Questions

On 10 June 2014, the Commission published the Financial Crime Guidance Note – Visit Trends and Observations. Section 5 of the Note identified examples of good and poor practice in relation to the preparation of a BRA. The Note also lists some questions intended to assist a business in assessing whether its approach in preparing and reviewing a BRA is appropriate and effective.

A business should therefore consider asking itself the following questions after it has prepared its initial BRA and after undertaking a review of an existing BRA, before it is finalised:

- Can the business clearly explain what it considers to be its greatest area(s) of risk exposure in relation to financial crime?
- How does the business risk assessment inform the overall risk appetite of the business?
- Has the business identified the risks associated with its customer base, products and services, its geographical areas of operation and delivery channels? (e.g. internet, telephone, branches).
- How does the business risk assessment inform the compliance policies, procedure and controls designed to mitigate the financial crime risks to which it could be exposed?
- Does the business take account of the level of compliance resources currently available and whether these are suitable and sufficient with regard to the financial crime risks identified and assessed?
- What information is relied upon by the Board when it reviews its business risk assessment in order to assess the financial crime risks to which it could be exposed?
- Does the business consider the risks identified when it reviews its business risk assessment, in the round, in order to determine whether the possible level of risk exposure might actually be higher than when each of the risks is identified in isolation? (i.e. is the accumulation of the risks / possible confluence of those risks considered in determining the overall risk appetite of the business?)

New Requirement – Submission of Draft BRA

With effect from Friday 5 September 2014, a draft BRA, prepared in compliance with Regulation 3 of the AML/CFT Regulations and the rules in Chapter 3 of the Handbook, must be submitted with any application for a licence or registration under the laws. Further information about this requirement can be found on the Commission's News webpage.

Sources of Information

The following are just some of the sources of information which can be accessed in order to better understand the types of financial crime risks to which a business may be exposed.

- FATF, Risk-based Approach, Guidance for Money Services Businesses, July 2009
- FATF, Guidance for a Risk Based Approach, Prepaid Cards, Mobile Payments and Internet-based Payment Services, June 2013
- JMLSG, Guidance for Money Services Businesses (as customers of banks), 20 May 2014
- JMLSG, Guidance for Money Service Providers, 21 July 2014
- Basel Committee on Banking Supervision, Sound management of risks related to money laundering and financing of terrorism, January 2014
- IAIS, Application Paper on Application Paper on Combatting Money Laundering and Terrorist Financing, October 2013
- FATF, Best Practices Paper - The Use of the FATF Recommendations to Combat Corruption, October 2013
- FATF Guidance, Politically Exposed Persons (Recommendations 12 and 22), June 2013
- FATF, Guidance for a Risk-Based Approach to Pre-paid Cards, Mobile Payments and Internet-based Payment Services, June 2013

- FATF, Best Practices, Combatting the Abuse of Non-Profit Organisations (Recommendation 8), June 2013
- FATF, Guidance on the Risk-Based Approach for the Life Insurance Sector, October 2009
- FATF, Guidance on the Risk-Based Approach for Real Estate Agents, June 2008
- FATF, Guidance on the Risk-Based Approach for Accountants, June 2008
- FATF, Best Practices on Trade Based Money Laundering, June 2008
- FATF Guidance on the Risk-Based Approach for Trust and Company Services Providers (TCSPs), June 2008
- IOSCO, Anti-Money Laundering Guidance for Collective Investment Schemes, October 2005
- The Egmont Group of Financial Intelligence Units – Cases at www.egmontgroup.org/library
- The Wolfsberg Group at www.wolfsberg-principles.com.

Q: Can I Rely on a 3rd Party to Perform my AML Compliance Function?

Corporate Governance – Compliance Arrangements – Outsourcing

A business may outsource a function which forms a part of its compliance arrangements designed to deter, forestall and prevent financial crime. Guidance on the factors which a business should consider when entering into such an arrangement can be found in section 2.3 of the Handbooks.

This FAQ has been prepared to answer questions received by the Commission about these activities.

Engagement of External Service Providers

Regulation 15 of the AML/CFT Regulations requires that a business establish such policies, procedures and controls as may be appropriate and effective for the purpose of forestalling, preventing and detecting money laundering and terrorist financing ("compliance arrangements"). In certain instances, a business may outsource a part of those arrangements to a third party, either in Guernsey or overseas or within its group or externally ("External Service Provider").

Engagement of External Reviewers

Rule 28 of the Financial Services Businesses and rule 43 of the Prescribed Businesses Handbooks requires that the Board of a business consider whether it would be appropriate to have a separate audit function to assess the adequacy and effectiveness of its compliance. In lieu of this, some businesses engage the services of an external contractor, consultant or reviewer ("External Reviewer"), to review all or part of their compliance arrangements in order to determine whether they remain appropriate and effective in preventing, forestalling and detecting the specific financial crime risks to which the business may be exposed. This includes External Reviewers engaged to identify and then undertake remedial work on any deficiencies relating to customer due diligence, risk reviews or other similar matters.

Accountability for Outsourced Compliance Arrangements

Rule 27 of the Handbook states that the Board of a business has effective responsibility for compliance with the Regulations and the rules in the Handbooks. A business -cannot contract out of its AML/CFT statutory or regulatory responsibilities. The business remains responsible for ensuring that, whether using an External Service Provider or External Reviewer, its compliance arrangements are compliant with the AML/CFT Regulations and the Handbooks.

The Commission expects that a business will incorporate measures to ensure that its engagement of External Service Providers or External Reviewer allows its Board to satisfy the requirements of Regulation 15, rules 27 and 28 of the Financial Services Businesses Handbook and rules 43 and 44 of the Prescribed Businesses Handbook. These measures include:

- Steps are taken prior to engagement to verify that the external party is qualified, knowledgeable of the applicable AML/CFT requirements and sufficiently resourced to perform the required activities.
- The external party is screened in compliance with Chapter 11 of the Financial Services Businesses Handbook and Chapter 9 of the Prescribed Businesses Handbook.
- Outsourced work is undertaken in compliance with the requirements of the Handbooks and AML/CFT Regulations and that measures are in place to verify that this is the case, by the business.
- Reports or progress summaries must be provided to the business which contain meaningful, accurate and complete information about the activities undertaken, progress of work and areas of non-compliance identified so as to allow the business to comply with rule 30 of the Handbook, if required.
- Measures to ensure that an external party reports any suspicious activity to the MLRO of the business about any suspicious activity and provides the MLRO with all relevant information.
- Reports received from an External Reviewer explain in sufficient detail the materials reviewed and other sources investigated in arriving at its conclusions so as to allow the business to test or verify the findings made or conclusions drawn.

Relevance – Mitigation – Non-Compliance with Regulations or Handbooks

The fact that a business has relied upon an External Service Provider or the report of an External Reviewer will not be considered by the Commission to be a mitigating factor where the business has failed to comply with the AML/CFT Regulations and/or the Handbooks.

The onus is ultimately upon the business to determine the appropriateness of placing reliance upon an external party for performing any of its compliance functions or providing it with advice as to the appropriateness and effectiveness of its compliance arrangements.

Q: Certification of Copy Documentation Requirements and Best Practice

Introduction

Rule 100 of the FSB Handbook and rule 114 of the PB Handbook require that a business takes adequate measures to mitigate the specific risks of non-resident individual customers, to complement those which are required for face-to-face customers. One of these measures includes requiring additional documents.

Where the additional documents obtained are copies of original documentation, rule 101 of the FSB Handbook and rule 115 of the PB Handbook state that the business must ensure that the copy documents have been certified by a suitable certifier.

Purpose of Certification Requirement

The certification requirement is intended to ensure that the business is not provided with fraudulent or misleading documentation as part of the CDD being undertaken of a business relationship or occasional transaction. The successful use of an "unsuitable certifier" can allow criminals or terrorists to have copies of either stolen identity documents or fraudulently obtained identity documents certified to facilitate, for example:

- The formation of companies utilising fraudulently obtained certified identity documents, hiding the true identity of the criminal / terrorist; and
- The creation of "ghost accounts" (accounts opened utilising fraudulently obtained certified identity documents) through which proceeds can be funnelled.

Purpose of Certifier Requirement

The certifier should be a trusted third party who is providing assurance that the document is a true copy of an original document (or extract thereof) or that the document provided shows the true likeness of the individual, whom the certifier has actually met face to face.

Use of a certifier guards against the risk that identification data provided does not correspond to the individual whose identity is to be verified or the documentation which alleged to have been copied and upon which the business plans to rely.

Policies, Procedures and Controls

The effectiveness of this control depends upon the individual who has certified the documents having actually seen and verified the original documentation or having actually met the individual, as the case may be. Assessing the suitability of the individual who has certified the documentation is a critical component of ensuring that this control is effective and should be relied upon by the business.

As part of good practice, a business should have, as part of its compliance arrangements:

- A policy and procedures which reflect its risk appetite towards relying upon certified documents;
- Its policy in relation to those individuals whom it considers to constitute "suitable certifiers"; and
- Procedures to verify the suitability of those who have certified documents on which it intends to rely.

Nature of Certification

The basic requirements are described in sections 4.5.2 of the Handbooks. It is important that the staff of a business understand the difference between the certification required in relation to identification documents and other documents.

Documents which are provided to evidence the identity of an individual must be certified with the statement that the document is a true likeness of the subject individual. This means that the certifier must have met the individual on a face to face basis.

Businesses should not rely on copies of previously certified documentation which has been re-certified, unless it can verify that the current certifier has actually seen the original documentation or met the individual in question.

Suitability of Certifier

As part of its compliance arrangements relating to CDD, businesses must give consideration to the suitability of a certifier based on the assessed risk of the business relationship or occasional transaction, together with the level of reliance being placed on the certified documents (See Rule 103 of the FSB Handbook and rule 117 of the PB Handbook).

The Commission considers it to be good practice for a business, as part of its compliance arrangements, to have in place a policy and procedures, which explains its assessment process to determine whether an individual is "suitable", and therefore place reliance upon the certified material provided.

The risk appetite of the business should inform its policy in relation to which types of individuals it will consider to be suitable certifiers. Key to this is ensuring that there is a means by which the individual's

honesty and integrity can be relied upon, so that the risks of misrepresenting or fraudulently making the required certification, are minimised.

The types of factors that could be taken into account in making this assessment, include whether:

- The individual holds an appropriate public position with a high level of trust and for which background checks or similar vetting of their fitness and propriety has occurred (e.g. a member of the judiciary, customs officer, officer of an embassy, consulate or high commission of the country or territory who has issued the passport or ID, or a serving police officer);
- The individual is a member of a professional body which undertakes independent oversight of compliance with its own rules or standards of professional conduct (e.g. a lawyer, notary, actuary, accountant who is a member of a recognised professional body);
- The individual is required to satisfy criteria similar to the "fit and proper" requirements of the minimum licensing criteria in Guernsey and are required to be vetted or approved as part of the regulation in the jurisdiction in which it operates (e.g. director, partner, controller, persons holding a controlled function, MLRO, General Representative of a financial services business);
- The individual is employed by another business which forms a part of a group of which the business is also a member, where the same or equivalent AML/CFT policies procedures and controls apply;
- The individual is subject to other professional rules or member of an industry body (or equivalent) providing for the integrity of conduct; and
- The individual is not closely related to the person whose identity is being certified (e.g. immediate family member, spouse).

Businesses must also exercise caution, especially where such documents originate from a country or territory perceived by the financial services business to represent a high risk, or from unregulated entities in any country or territory.

Contents of the Certification

Rule 106 of the FSB Handbook and rule 120 of the PB Handbook require that a certifier sign and date the copy document and provide adequate information so that contact can be made with the certifier in the event of a query.

The Commission considers that as part of good practice, "adequate information" means:

- The full name of the certifier (i.e. not just the signature);
- The location where the document was certified (e.g. St Peter Port, Guernsey);
- The professional position or capacity held by the certifier;
- A contact telephone number; and
- An email address at which the certifier can be contacted.

This information may be provided either on the certified document or attached to that document by way of email or other record, which accompanies the certified document.

Verification Enquiries about a Certifier

Procedures should clearly explain the risk-based process by which verification of the identity and position held by the certifier should occur. The Commission considers best practice to include a greater degree of enquiry to be undertaken given:

- The risk profile of the business relationship or occasional transaction;
- The level of reliance being placed on the documents; and

- Whether the documents originate from a country or territory perceived to represent a high risk or in relation to an unregulated entity.

A business should also consider whether the degree of reliance to be placed in those cases where the certifier is not previously known to the business. Importantly, the capacity or position of the certifier should be independently verified.

It is also important to check on a risk-basis that where a certification relates to the true likeness of an individual, that the certifier has actually met the individual in person.

Ongoing Monitoring Measures

Businesses should consider, on a risk basis, as part of their ongoing risk relationship monitoring contacting a certifier to ascertain whether any circumstances have changed with respect to the subject individual which would change its known risk profile. This is particularly relevant where publically available information is not on offer by internet research or where there is no customer relationship manager involvement.

Electronic Certification

Businesses should be aware that the reliance upon alternative methods is a matter for their assessment based on their understanding of the veracity of the certification process.

Q: We Have Discovered that we Have Not Undertaken CDD in Compliance with the Requirements of the Regulations and/or Rules in the Handbook. We are Reluctant to Approach the Customer and Would Like an Exemption from Having to Comply with these Requirements.

A: The Commission does not have the power to exempt a business to whom the Regulations apply from complying with its requirements. Neither would it be appropriate for the Commission to provide its consent for a business to derogate from the rules in the Handbook. The rules are specifically designed to assist businesses in complying with the requirements of the relevant legislation concerning money laundering, terrorist financing and related offences to prevent the Bailiwick's financial system from being used in the laundering of money or the financing of terrorism.

The Commission expects that a business will take a risk-based approach in considering the steps that should be taken by it, in the absence of compliance customer due diligence having been undertaken, to mitigate the financial crime risks to which it could otherwise be exposed prior to processing the transaction. The Commission would expect that a member of the business' compliance staff are alerted and advice sought from them, beforehand.

The decision whether to proceed with the transaction should be recorded. The record should evidence the measures taken and controls applied to mitigate the associated financial crime risks. Businesses should also be conscious that the circumstances could also lead to the forming of a suspicion for which a SAR should be made.

The Commission would encourage businesses to engage with the Financial Crime Supervision and Policy Division in such circumstances, and should be mindful of the requirements of rule 30 of the Financial Services Businesses Handbook and rule 46 of the Prescribed Business Handbook. These rules require that the board of a business, or equivalent, ensure that the Commission is advised of any material failure to comply with the provisions of the Regulations and the rules in the Handbook, and of any serious breaches of the policies, procedures and controls of the business.

Q: Why Have the Handbooks Not Been Updated to Include the New Al-Qaida (Restrictive Measures) (Guernsey) Ordinance 2013 ("the 2013 Ordinance")?

A: The Handbooks for Financial Services Businesses on Countering Financial Crime and Terrorist Financing and for Legal Professionals, Accountants and Estate Agents on Countering Financial Crime and Terrorist Financing (collectively known as "the Handbooks") include both the full text of the repealed Al-Qaida and Taliban (Freezing of Funds) (Guernsey) Ordinance, 2011 and paraphrased text clarifying the actions required of firms to meet their reporting obligations.

The Handbooks were updated in March and April 2013 following extensive consultation with industry. The 2013 Ordinance came into force on 27 August 2013, several months afterwards.

The Commission has commenced work on the review and re-assessment of the two Handbooks and their contents. A working group has been engaged in these activities since October 2013. The Commission determined that as a result of the work being undertaken, it would not be appropriate for further revisions to be made to the Handbooks until the revision work has been completed, but is taking steps to ensure that this work includes an update which confirms that the 2011 Ordinance has been superseded and replaced by the 2013 Ordinance.

The Commission has explained at a number of public presentations to industry that further points of clarification, correction or replacement of text within the Handbooks will be addressed through the FAQ webpage or separate correspondence, until the proposed amendments to the Handbooks are circulated for broader consultation.

Q: Is it Necessary to Appoint a Nominated Officer and/or a Deputy MLRO and Do They Need to be a Member of Management?

A: Businesses are required under the Regulations and the Handbook to appoint an individual to act as Money Laundering Reporting Officer ("MLRO") and another individual as its Nominated Officer, to receive disclosures from staff in the absence of the MLRO.

Chapter 2 of the Handbooks contains rules concerning the roles of both "MLRO", any deputy MLROs that are appointed and Nominated Officers. Regulation 12 specifically requires that the individual appointed as MLRO must be of at least management level, and the rules in Chapter 2 also require that the Nominated Officer also be of at least management level.

A business may, but is not required by the Regulations or Handbooks, to appoint a Deputy MLRO. If a business elects to appoint a Deputy MLRO, the rules in Chapter 2 of the Handbook require that the individual be a Guernsey resident and be empowered with specific duties, which include direct access and contact with the Board. The level of responsibility of a Deputy MLRO and Nominated Officer therefore necessitates that the individual appointed to that position be of a suitable seniority level that will enable them to fulfil these duties in an unimpeded manner.

When selecting an individual for the position of Deputy MLRO or Nominated Officer, businesses should also be mindful of the screening and training requirements in the Regulations and Handbooks, given the critical decision making role played by them in mitigating the risk of exposure to any money laundering and terrorist financing risks.

Q: Do Reliable Introducer Relationships Need to be Tested Annually Do I Have to Visit Introducers I Rely Upon as Part of Our Testing Programme?

A: The Handbook does not prescribe frequency or manner in which testing is undertaken.

A business must recognise that introduced business by its very nature has the capacity to be high risk and a financial services business must use a risk-based approach when deciding whether it is appropriate to rely on a certificate or summary sheet from an introducer in accordance with Regulation 10 or whether it considers it necessary to do more.

The Handbooks' rules require that a business have a programme of testing to ensure that introducers are able to fulfil the requirement to provide certified copies or original documentation upon request and without delay.

It is expected that a business will adopt a risk based approach when designing its system of testing. The expectation is that the programme acts as an appropriate and effective control that allows a business to be confident that it can continue to rely upon the introducer to fulfil the obligations to which is has certified.

The scope of testing undertaken should include verification that the information received on the requested certificate or summary containing information about the underlying customer or beneficiary continues to be accurate and up to date. This allows the business to determine whether, based on any changes, it wishes to continue to rely upon the arrangement or whether the business may wish to seek further information from the introducer about the underlying customer.

Q: What is considered acceptable evidence for source of funds and wealth?

A: Regulation 5 defines enhanced due diligence as including the taking of reasonable measures to establish any source of funds and the wealth of a customer, beneficial owner and any underlying principal.

Enhanced due diligence is intended to ensure that businesses have a better understanding of the risks associated with high risk customers so as to enable them to decide whether to establish or continue with the business relationship and to mitigate any risk of money-laundering. Enhanced due diligence also forms a basis for a business' understanding of its customer's affairs. Understanding the legitimacy of a customer's source of funds and wealth is a critical component of customer due diligence, especially in relationships with politically exposed persons.

Ascertaining the legitimacy of the monies is achieved through evidencing responses from customers to enquiries about their source of funds and wealth. The extent of enquiry and the level of evidence obtained should ascertain the source of the funds and how they were generated.

The Handbooks and Regulations do not prescribe the measures that must be taken by a business in this respect, however some examples have been included below.

It would not be considered a reasonable measure for a business to accept customers' responses on an application form at face value particularly where vague responses are given (i.e. "employment and salary") without further clarification as to where the customer was employed and their actual level of income, for example. The Commission would expect the business to have obtained information, such as a copy of a pay slip, tax return etc. to establish the legitimacy of the source from which a client has told them that funds or wealth originated. This information should then be incorporated into the documented consideration required by the Handbooks' rules to be made of the risk implications of the source of the funds and wealth and geographic sphere of the activities that generated them.

Understanding the source of a customer's funds is an on-going requirement and applies to all new proceeds passing through the relationship. Monitoring undertaken as part of enhanced due diligence should include assessing on an ongoing basis whether the transactional activity of that relationship is consistent with the risk profile of that customer, including its source of wealth.

Source of Funds Examples of Evidence

Income from Employment (i.e. wages, bonus)

- An original or certified copy of a recent pay slip
- Written confirmation of annual salary signed by employer

Property Sale

- Original or certified copy of contract of sale
- Written confirmation of sale signed by advocate/solicitor

Sale of Investments

- Original or certified copy of contract note/s
- Written confirmation of sale/holding signed by accountant/ broker

Inheritance

- Original or certified copy of Will or Grant of Probate
- Written confirmation of inheritance signed by advocate/solicitor/trustee/executor

Company Sale

- Original or certified copy of contract of sale
- Written confirmation of sale signed by advocate/solicitor/ accountant
- Internet research of Company Registry

Divorce Settlement

- Original or certified copy of court order
- Written confirmation of settlement signed by advocate/solicitor

Savings

- Statement from the savings institution and enquiry of the source of wealth

Lottery/ Gambling win

- Evidence from the lottery company
- Cheque
- Winning's receipt

Q: Following the amendments made to the Handbook this year, what are the AML/CFT obligations of a general insurer?

A: Intelligence and information in the jurisdiction identified that there was a very low risk of general insurance products being used to launder the proceeds of crime or terrorism. As a result, amendments were made to the relevant legislation so that the AML/CFT requirements in the Regulations and the Handbook would no longer apply to general insurers.

Long-term insurers, insurance intermediaries advising on or arranging long-term insurance products and insurance managers licensed under the Insurance Law, must still comply with the AML/CFT Regulations and the Handbook.

Despite the above amendments, general insurers must still comply with the requirements in other Financial Crime legislation. This includes the disclosure requirements of The Disclosure (Bailiwick of Guernsey) Law, the Terrorism and Crime (Bailiwick of Guernsey) Law and the Drug Trafficking (Bailiwick of Guernsey) Law.

General insurers must also continue to comply with the requirements, reporting and restrictions imposed by the UN, EU and other bodies concerning sanctions. This includes Ordinances such as the Al Qaida (Restrictive Measures) (Guernsey) Ordinance, 2013. General insurers must also comply with The Prevention of Corruption (Bailiwick of Guernsey) Law.

The Licensed Insurers' Corporate Governance Code General Insurers requires that general insurers comply with the above legislation and establish an appropriate internal control system with procedures to ensure that this occurs.

Q: What is Meant by the Term 'Object of a Power' and When Must Customer Due Diligence be Undertaken?

A: The term "object of a power" refers to an individual or party who, although not expressly identified in a trust instrument or by law, as a beneficiary, could benefit from the trust if the trustee were to exercise its powers for this purpose. An example of this could be in the case of a discretionary trust where the settlor has issued a letter of wishes to the trustee, identifying an individual whom they would wish to receive proceeds from the trust. The term is therefore intended to refer to parties who might otherwise benefit from the trust, depending upon whether those with power to make such a determination, exercise those powers in their favour.

<u>Customer Due Diligence ("CDD") on Objects of a Power</u>

Where the identity of an object of a power has been made known to the trustee (such as in a letter of wishes or through correspondence with the settlor), the trustee should ensure that information regarding the object's identity is recorded and that CDD in compliance with the Regulations and Handbook, is conducted at the earliest opportunity. This is not intended to require a trustee to guess or estimate the likelihood of those falling within a class or group whose identity is not known to the trustee at the time the relationship is established.

The trustee, as the party with the ability to exercise this power, must assess in a reasonable manner whether it is likely to do so in relation to an individual or party. Where it determines that it is likely to do so, the trustee must take steps to undertake CDD at the earliest opportunity on the individual or party. The Commission would therefore expect a trustee to have undertaken CDD on an object of a power once this has been determined. It is understood that a trustee may make this determination at the time the business relationship is established or at a later period thereafter. The Commission expects that in those latter instances, the trustee will have taken steps to ensure that controls are in place to prevent the distribution of assets to (or on behalf of) an object of a power taking place until CDD has been completed in compliance with the Regulations and the Handbooks (See Regulation 7).

There may also be instances where circumstances preclude a trustee from obtaining CDD directly from an object of a power. One example might be where the settlor requests that the existence of a trust be kept confidential from those individuals identified in a letter of wishes until the trustee decides to exercise its powers in their favour. In these circumstances and where the relationship has been assessed as high risk, the Commission expects that the trustee will endeavour to verify the identity of the object of a power through other means at the time the assessment of risk is made.

In any event, the trustee must ensure that controls are in place to prevent the distribution of assets to (or on behalf of) the object of a power until the necessary CDD has been completed in compliance with the Regulations and the Handbooks.

Record Keeping

Records should be maintained by the trustee regarding objects of a power, the circumstances giving rise to CDD not being collected, and the controls put in place to prevent proceeds being paid until the required CDD has been completed.

The Commission will not consider a trustee to have complied with the Regulations and the Handbooks where it has deferred the collection of CDD on an object of a power until prior to a distribution taking place, in the absence of a recorded explanation of why this was not possible.

Introducer Arrangements

Where a trustee has provided another financial services business with an introducer certificate, the Commission would expect that the trustee take steps to notify the holder of an introducer certificate of any objects of a power it has identified, either in the certificate summary if known at the time the certificate is issued, or at any time thereafter when the trustee determines that it is likely to exercise its powers in favour of that individual.

The trustee should also ensure that it makes the certificate holder aware of any circumstances as a result of which the trustee has not been able to conduct CDD on the object of a power it has identified in the certificate and the controls it has put in place to reduce the risk of proceeds being paid to that individual until such time as the CDD has been obtained in compliance with the Regulations and the Handbooks.