Guernsey Financial Services Commission

Financial Crime Supervision & Policy Division

Guidance Note

Visit Trends & Observations

January 2012 - 30 March 2014

1. INTRODUCTION

This Guidance Note ("Note") has been prepared following analysis by the Commission of both the results of onsite visits undertaken since 2012, along with trends that have been identified from financial crime assessments undertaken at the international level.

This Note is intended to further assist businesses in understanding the Commission's expectations in relation to their compliance with the requirements of the Regulations and the rules in the Handbooks.

Businesses may adopt other appropriate and effective measures to those described in this Note, provided that they can demonstrate that those measures also achieve compliance with the Regulations and rules in the Handbooks.

This Note does not touch upon all of the requirements of the Regulations and rules in the Handbooks, nor is the content of this Note intended to amend, substitute, supersede or replace these rules and requirements.

The trends and observations identified in this Note are in addition to those matters identified in the "Dear CEO" letter issued by the Commission on 27 May 2014, and the Instruction issued to licensed fiduciary businesses on 28 May 2014. Reference should therefore be made to these documents, along with any FAQs, additional Instructions and other information provided by the Commission about financial crime on its website.

The Commission will consider the practices listed in this Note during on-site visits and will also be considering these as part of the current review and amendment of the Handbooks being undertaken by the joint Commission and industry working group.

Businesses are reminded of their obligations in rule 30 of the Handbook for Financial Services Businesses and rule 46 of the Handbook for Legal Professionals, Accountants and Estate Agents, on Countering Financial Crime and Terrorist Financing. This rule requires that a business ensure that the Commission is advised of any material failure to comply with the Regulations and the rules in the Handbooks or any serious breaches of the policies, procedures and controls of the business.

Samantha J Sheen
Director
Financial Crime Supervision & Policy Division

10 June 2014

DEFINITIONS

References to "**Board**" include any equivalent body i.e. Partners or Principals of the business.

References to "**business**" include both prescribed businesses and financial services businesses, as those terms are defined in the Regulations.

References to "**financial crime**" include money laundering, terrorist financing, bribery and corruption, tax evasion and other predicate offences as listed in Chapter 1 – Section 1.1 Background and Scope - of the Handbooks.

References to the "**Handbooks**" in this Note relate to the Handbook for Financial Services Businesses on Countering Financial Crime and Terrorist Financing and the Handbook for Legal Professionals, Accountants and Estate Agents on Countering Financial Crime and Terrorist Financing.

References to "**MLRO**" includes Nominated Officers.

References to the "**Regulations**" in this Note relate to The Criminal Justice (Proceeds of Crime)(Financial Services Businesses)(Bailiwick of Guernsey) Regulations, 2007 and The Criminal Justice (Proceeds of Crime) (Legal Professionals, Accountants and Estate Agents) (Bailiwick of Guernsey) Regulations, 2008, both as amended.

All other terms used in this Note are as defined in either the Regulations or Handbooks, where so defined.

SELF-ASSESSMENT QUESTIONS:

These questions are intended to assist a business in assessing whether its approach is appropriate and effective.

The Commission may follow similar lines of inquiry when discussing financial crime matters during on-site visits.

The questions are not intended to be exhaustive. Businesses should consider the most suitable means by which to assess the appropriateness and effectiveness of their compliance arrangements.

Examples of good practice:

- These examples present some, but not all, of the ways in which a business might comply with the Regulations and rules in the Handbooks.
- These examples are non-exhaustive. The Commission would draw comfort from seeing evidence that these practices, given the nature, size and complexity of the business have been applied.

Examples of poor practice:

- These examples present some, but not all, of the ways in which a businesses have failed to comply with the Regulations and rules in the Handbooks.
- These examples are non-exhaustive and do not identify all cases where conduct may give rise to regulatory breaches or criminal offences.

2: CORPORATE GOVERNANCE

Self-Assessment Questions:

- How is the Board kept up to date on financial crime issues? (this may include receiving reports on the business' performance in this area as well as ad-hoc briefings on individual cases, emerging threats or legislative changes).

- When did the Board, including appropriate sub-committees (where applicable), last consider financial crime issues? What action followed the discussions undertaken?

- Where compliance and/or MLRO reports are presented to the Board, is the Board's consideration of the report'(s) contents recorded in the minutes?

- Is the reporting made to the Board meaningful and relevant? (e.g. does it simply comprise of a series of figures from one quarter to the next, or does it include analysis and summaries of key findings, accompanied by recommendations in response to those findings?).

- How does the Board gain assurance that outsourced compliance functions are being undertaken by the provider in compliance with the requirements of the Regulations and the rules in the Handbook?

- Are Board members sufficiently familiar with the business risk assessment and the business' compliance arrangements in order to oversee and review these arrangements, when required?

- Through what means does the Board determine whether its oversight of the business' compliance arrangements are appropriate and effective?

✓	✘
Examples of good practice:	**Examples of poor practice:**
• The Board meets on a regular basis to allow it to consider in timely manner a review of its business risk assessment, compliance arrangements, or measures proposed in response to the findings from ongoing monitoring and customer risk reviews. • Board reporting about compliance arrangements of the business is timely, accurate and meaningful. • Board and sub-committee meeting materials, including minutes, evidence that financial crime-related reports are reviewed, challenged and discussed. • There is demonstrable evidence that the compliance officer and MLRO have unfettered access to the Board. • The Board and senior management have a demonstrable awareness of financial crime risks and are supportive of strong preventative measures. This includes, where warranted, the rejection of high-risk business and/or closing of existing accounts. • The Board and relevant employees of the business understand the obligations of rules 30 and 46 of the Handbooks and take steps to ensure that the Commission is advised in a timely manner of any material failure to comply with the Regulations and the Handbooks, or any serious breaches of its own policies, procedures and controls. • The Board and the relevant employees of the business are fully engaged around the results of Commission onsite visits, and actively oversee the timely completion of required remediation measures to prevent reoccurrence.	• The Board fails to meet on a regular basis in order to consider, review and oversee its business risk assessment and compliance arrangements and implement measures proposed in response to the findings from on-going monitoring and customer risk reviews. • Board reports do not provide meaningful and complete information about the effectiveness of compliance arrangements and the financial crime risks to which the business may be exposed. • Neither the contents of verbal reports nor discussions regarding financial crime matters are recorded in the Board minutes in a complete and accurate manner. • Little weight is given or significance attributed to the reports or advice provided by the MLRO about concerns arising from a high risk rated customer and how this should be addressed by the business. • Commercial benefit overrides the use of strong preventative measures. High risk business is taken-on or retained without the approval of the Board or senior management and without having verified whether the business can effectively mitigate the associated financial crime risks. • Where compliance concerns have been identified during a Commission onsite visit, no effective oversight is undertaken to ensure that required remediation measures are undertaken and completed in a timely manner to prevent reoccurrence.

3: POLICIES AND PROCEDURES

Self-Assessment Questions:

- How soon after the review and revision of its business risk assessment, does the business review its compliance policies, procedures and controls, taking into account its size, nature and complexity?
- Who is responsible for reviewing the compliance arrangements of the business?
- When were the business' compliance arrangements last reviewed?
- What measures were used by the Board to determine the appropriateness and effectiveness of the business' policies, procedures and controls which comprise its compliance arrangements?
- How are the results of the review reported to the Board?
- How does the business ensure that its policies, procedures and controls are disseminated to its staff, outsourcing providers and group entities, and are therefore applied?
- What steps does the business take to ensure that staff understand its compliance policies?
- Procedures and controls and any changes that are subsequently made to them?

✓

Examples of good practice:

- The business is able to demonstrate how its business risk assessment informs the compliance arrangements implemented by the business to mitigate the financial crime risks to which it could be exposed.
- Compliance policies, procedures and controls are designed to address the financial crime risks to which the business would be exposed, in compliance with the Regulations and the rules in the Handbook.
- Compliance policies procedures and controls are regularly reviewed and updated following any revisions or updates to the business' business risk assessment, the Regulations, the rules in the Handbook and any instructions or guidance issued by the Commission from time to time.
- A business' review of its compliance arrangements includes sampling to verify whether its staff and outsourcing service providers are implementing policies, procedures and controls in the required manner.

✗

Examples of poor practice:

- There is no demonstrable connection between the compliance policies, procedures and controls of the business and the risks assessed in its business risk assessment.
- Compliance policies, procedures and controls are generic in nature and do not facilitate the business' compliance with the Regulations and the rules in the Handbook.
- The requirements of the business' policies, procedures and controls do not appear to align with the actual practices being applied by the staff of the business.
- Policies, procedures and controls are not reviewed in a timely manner following the revision or updates to the business risk assessment, the Regulations, the rules in the Handbook and instructions or guidance issued by the Commission from time to time.
- Staff feedback given on the difficulties of implementation or conflicts with other operating requirements of the business' compliance arrangements, yet no steps are taken to review policies, procedures and controls to ensure that staff can actually implement them, as intended.

4: THE MONEY LAUNDERING REPORTING OFFICER

Self-Assessment Questions:

- How does the business, as part of its compliance arrangements, assess whether its MLRO has sufficient resources and access to records to perform his or her duties effectively?
- Is there interaction between the staff and the Board with the MLRO on matters relating to financial crime?
- Does the MLRO escalate relevant matters to the Board and senior management?

✓

Examples of good practice:

- The MLRO is independent and is able to pose effective challenge to the business where warranted.
- The MLRO receives full cooperation from all staff.
- The MLRO regularly undertakes training with all staff on financial crime risks which are specific to the business, its customer base and its products and services.
- The MLRO verifies that enhanced training is undertaken by the Board and senior management on financial crime matters.
- The MLRO maintains readily retrievable records of all the decisions made on SARs, whether they were reported to the FIU, together with the reasons when they were not reported.
- The MLRO assesses the SARS received and makes a timely decision whether to make a disclosure report to the FIU, and ensures that appropriate controls are placed on the customer's account, where required.

✗

Examples of poor practice:

- The MLRO is responsible for business development or customer relationships and is conflicted when SARs are received regarding the customers for which the MLRO is responsible.
- The MLRO encounters difficulty obtaining information due to a lack of cooperation offered by customer relationship managers and front line staff.
- The MLRO is insufficiently resourced to provide up-to-date and relevant training in financial crime matters.
- The MLRO does not have regular contact with the Board and is not is not aware of his obligations to the business under the Regulations or the rules in the Handbook.
- The MLRO limits the records it maintains to the date and staff member from whom SARS are received and is unable to accurately recount the reasons why he or she decided not to make a disclosure report to the FIU, when asked by a Competent Authority.
- The MLRO fails or postpones its assessment of SARs due to work commitments or pressure imposed by members of senior management responsible for maintaining the customer relationship.

5: BUSINESS RISK ASSESSMENT

Self-Assessment Questions:

- Can the business clearly explain what is 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 be 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?)

✓

Examples of good practice:

- The business prepares an assessment which is specific to its activities and relative to the size, nature and complexity of the business.
- The business has an overall risk appetite statement or standard, driven by its business risk assessment, which informs its business activities.
- The business risk assessment is reviewed on a scheduled basis and when events occur which may change the level of financial crime risk exposure to the business.
- The Board takes ownership for overseeing the timely review of the business risk assessment, which is appropriately delegated, taking account of the necessary resources and expertise.
- The results of the business risk assessment informs the compliance arrangements used by the business to mitigate the financial crime risks to which it could be exposed, and supplement, where applicable, assessments performed by parent or group entities.
- The business risk assessment takes account of any outsourcing arrangements and how these may impact upon its financial crime risk exposure and the controls that might be needed to mitigate those risks.

✗

Examples of poor practice:

- The business applies a template risk assessment which does not take account of the financial crime risks specific to its business activities.
- The business risk assessment is allowed to become outdated due to a lack of appropriate review by the Board and no longer reflects the current activities of the business and their corresponding financial crime risks.
- Where delegated, the business is unable to clarify whom is accountable for ensuring that a review is undertaken of the business risk assessment and reporting the results of that review to the Board.
- A Guernsey branch or subsidiary relies upon a group risk assessment without considering the specific financial crime risks to which the Bailiwick business could be exposed.
- Where compliance arrangements are outsourced, the business fails to assess whether these arrangements may impact upon its financial crime risk exposure and the controls that may be needed to mitigate those risks.

6: CUSTOMER RISK ASSESSMENT

Self-Assessment Questions:

- What specific factors are considered by the business to assess the particular financial crime risks that may be posed by a customer? (i.e. their wealth, their influence, their geographical origin, the products and services offered by the business and the value of transactions)

- What measures are used by the business to undertake a customer risk assessment? (i.e. forms, on-line systems). Do these encourage a meaningful overall assessment of a customer's risk profile?

- What is the process of assurance around the assignment of risk ratings? Who is authorised to assign risk ratings and what measures are in place to verify the accuracy of the ratings assigned?

- Is consideration given to both the individual risk profile characteristics of a customer and how those characteristics might escalate the level of potential financial crime risk exposure (i.e. the accumulation of risk and confluence of risk), before a risk rating is assigned?

- Is consideration given to the cumulative effect of financial crime risks, which can occur where a customer's risk profile comprises of introduced business (i.e. non face-to-face relationships) complex structures and the use of nominees for example?

- Is the outcome of a customer risk assessment recorded so that it is readily accessible for the purposes of ongoing monitoring and customer risk reviews?

- Through what means has the business determined that its customer risk review process is appropriate and effective?

✓

Examples of good practice:

- There are clear policies, procedures and controls in place which explain the process to be followed in conducting a customer risk assessment.
- The business' risk classification system is informed by the Regulations, the rules in the Handbook, guidance and instructions issued by the Commission from time to time and the business' own risk appetite, as informed by its business risk assessment.
- The assessment recorded includes information concerning all of the risk profile characteristics considered including type, volume and value of expected customer activity, particularly for high risk customers, the purpose and nature of the relationship, the information relied upon by the business and the rationale for the risk rating assigned. The information recorded by the business is detailed, meaningful and accurate.
- The business understands the confluence of risks that may arise from the use of complex structures and non-face-to-face relationships and assigns a risk rating commensurate with the level of risk arising.

✗

Examples of poor practice:

- Information relating to the customer's risk profile is maintained in various formats and located in different systems or areas of the business, with no recorded rationale for the risk rating assigned.
- A customer risk classification is designed in order to avoid rating any customers as 'high risk' in the interests of maximising customer take-on and avoiding enhanced due diligence requirements.
- Risk assessment procedures comprise of a checklist, and recitation of the requirements of the Regulations and rules in the Handbook, without consideration of the business' risk assessment.
- No record is maintained as to the customer's rationale in selecting the Bailiwick to obtain the requested products and services, or the level of activity expected of the customer.
- Customer risk profile characteristics are assessed in isolation of one another without regard for the overall risk which the relationship could pose, particularly in the case of non-face-to-face relationships involving complex structures.

7: CUSTOMER DUE DILGENCE ("CDD")

Self-Assessment Questions:

- Do the policies and procedures concerning required CDD measures apply due diligence appropriate to the assessed risk?
- Do the CDD policies and procedures provide the business as a whole and the staff, in particular, with a clear understanding of the types of risks that are associated with individual business relationships?
- How does the business identify and verify the identity of beneficial owner(s) in the case of a non face-to-face business relationship?
- What steps are taken to verify the intended nature and purpose of the structures used by a customer where corporate, trust, foundation or other arrangements are used?
- What controls are in place to reduce the risks associated with placing reliance upon certified documentation for CDD purposes and, in particular, the risk that the business may rely upon false documentation?
- Through what measures has the business determined that its CDD policies and procedures are appropriate and effective?

✓

Examples of good practice:

- Robust procedures are consistently applied by the business to ensure that third parties are legally authorised to act for and on behalf of the customer. Appropriate risk-based CDD is undertaken by the business prior to accepting instructions from this party.
- The business understands and documents the ownership and control structures (including the reasons for any complex or opaque corporate structures) of clients and their beneficial owners.
- The business obtains sufficient information about the purpose and intended nature of the business relationship in order to be satisfied that it understands the associated money laundering risk.
- With regard to complex corporate structures, the business conducts CDD at all levels of each structure until it is satisfied that the corporate structure makes economic sense, having verified the legality of each entity and the identity of all beneficial owners and controllers.
- Information is routinely collected on the business and economic profile of each customer at the outset of the business relationship.
- The business has procedures, which are consistently applied by its staff, to ensure that copy documentation is certified in compliance with the rules in the Handbooks and that it considers the basis upon which the certifier was determined to be suitable.

✗

Examples of poor practice:

- CDD is not undertaken on third parties who are held out as being authorised to act for or on behalf of a customer.
- Over-reliance on a checklist to simplify CDD measures, regardless of the nature of the customer's risk profile characteristics.
- Inadequate CDD is undertaken because reliance is placed on the personal relationship held with the customer by a member of senior management or another influential customer of the business.
- Failure to ensure that verification of identity is completed as soon as reasonably practicable after a relationship is established, where reliance is placed on the exception provided for in Regulation 7 and Chapter 4 of the Handbooks.
- Relationships are established despite the refusal by the customer to provide the requested CDD.
- Reliance is placed upon photocopies of copy documentation certified by a third party at an earlier date for a purpose unrelated to the current transaction or business relationship.
- Reliance is placed upon CDD documentation which is provided in a language other than English, for which no translated version is obtained and reviewed.
- Inconsistencies between the CDD information provided by the customer and information found on publically available sources are not investigated prior to the take-on of the relationship.

✓

Examples of good practice continued…

- Robust procedures are in place and endorsed by senior management and the Board to prevent the take-on of relationships or processing of occasional transactions where inconsistencies in a customer's CDD have been identified.
- There are effective ongoing monitoring measures in place to track any outstanding or deficient CDD and demonstrable means undertaken to address them in a timely manner.
- The business undertakes a review of its compliance arrangements including sampling customer records in order to verify whether forms and applications are being used and completed in the required manner.
- Where a business fails to complete CDD in a timely manner due to the customer's refusal to provide the required information, it ensures action is undertaken in accordance with Regulation 9 and Chapter 4 of the Handbooks.
- The business rejects a transaction when a customer refuses to provide requested CDD.
- Rejected business is recorded where a new customer is unwilling to provide CDD and consideration is given to submitting a disclosure to the FIU.

✗

Examples of poor practice continued…

- Identified deficiencies in CDD are not followed up on, nor are controls put in place to mitigate the risks that could arise until those deficiencies are resolved.
- Controls such as forms and applications, intended to collect CDD information, are not scrutinized prior to accepting a business relationship to verify whether all required information has been provided.
- The business maintains a business relationship despite deficient CDD and repeated refusal by the customer to provide the requested information.
- The business culture favours keeping a new customer "sweet" by not requesting CDD information about the customer, in lieu of rejecting that relationship.
- Rejection of new business or transactions on CDD grounds is treated as a commercial decision, for which no record is maintained.

8: ENHANCED CUSTOMER DUE DILIGENCE ("EDD")

Self-Assessment Questions:

- How is EDD information gathered, analysed, used and recorded?
- What measures are in place to ensure that EDD is complete and that approval has been sought from senior management, prior to establishing a business relationship or undertaking an occasional transaction?
- What are the business' policies, procedures and controls concerning the take-on of customers who are a PEP or have an association with a PEP?
- What measures are in place to mitigate the risk that EDD is not completed, prior to approval being sought from senior management?
- How does the business ensure that its policies, procedures and controls are disseminated to its staff, its outsourcing service providers and group or parent entities about its EDD requirements?
- What steps does the business take to ensure that staff understand its compliance policies, procedures and controls relating to EDD and any changes that are subsequently made to them?
- What measures are used by the Board to determine whether its policies, procedures and controls concerning EDD are appropriate and effective?

✓

Examples of good practice:

- There is a clear line of accountability for the approval of high risk rated business relationships and occasional transactions. The MLRO and Compliance have adequate oversight of all high-risk relationships.
- Verification enquiries are undertaken using commercial databases and independent public sources to verify the identity of customers who are PEPs or are associated with a PEP.
- Senior management have received appropriate training and have a working knowledge of financial crime risks, which can be applied when considering whether to approve the take-on of a business relationship.
- Senior management responsible for approving high risk customer take-on are provided with sufficient time and resources with which to consider and assess customers and their overall risk profile.
- Measures are undertaken by the business to verify and document the source of wealth and source of funds for all high-risk rated business relationships, prior to being approved by senior management and take-on.
- The business has policies, procedures and controls to ensure that it is appropriate to rely on EDD performed by other entities in the same group.
- Client profiles for high risk customers are detailed, meaningful, accurate and regularly updated in order not to undermine the proper application of the ongoing monitoring process. The purpose of the business relationship is identified and recorded.

✗

Examples of poor practice:

- Approval of high risk rated relationship take-on or transaction activity is delegated by senior management to operational staff or those responsible for managing the commercial aspects of the relationship.
- Reliance is placed on the customer to identify for the business, through the completion of a new business or application, whether it is, or has, any association with a PEP.
- Responsibility for the approval of high risk customer take-on is delegated to members of senior management with limited training and understanding of the EDD requirements of the Regulations, the rules in the Handbook and the business' policies, procedures and controls.
- Senior management lack the necessary knowledge, time and resources to fully assess and verify whether EDD has been undertaken in full, prior to approving its take-on.
- The business does not distinguish between the customer's source of funds and their source of wealth and relies solely upon the information provided by the customer, without conducting any independent verification of that information.
- Reliance is placed on intra-group introductions where EDD requirements are not equivalent to those in the Regulations and the rules in the Handbook.
- Waivers are granted to staff conducting EDD, relieving them from establishing source of funds, source of wealth or other due diligence.

9: HIGH RISK RELATIONSHIPS

Self-Assessment Questions:

- Which members of senior management are authorised to approve the take-on of high risk relationships?
- To what extent do senior management have a working understanding of financial crime risks generally and those to which the business could be exposed?
- What roles does the compliance function of the business play in advising, assessing or assisting senior management in determining whether or not to take-on a customer rated as high risk?
- How does the business monitor high risk customer relationships? How does this differ from the monitoring of other relationships?
- How does the monitoring program allow for the business to identify, in a timely manner, when one of its existing customers subsequently becomes a PEP or acquires risk profile characteristics of a high risk nature? What procedures are in place to ensure that the risk rating of the customer is revisited, where this occurs?
- Has training been provided to staff on the risks associated with PEP customers and how the policies, procedures and controls of the business are designed to mitigate these risks?
- Through what means has the business determined that its policies, procedures and controls are appropriate and effective to mitigate the financial crime risks associated with high risk customers?

✓	✗
Examples of good practice: • There are clear procedures on the take-on of high risk customers for both business relationships and occasional transactions. These procedures are endorsed by the Board and senior management and consistently applied by the staff. • The review of compliance arrangements takes account of the available resourcing to conduct enhanced monitoring and review of high risk customers. • Where monitoring or a review suggests possible criminal conduct engaged by the customer, the business takes additional measures. These are undertaken in a timely manner and include supplementing enhanced due diligence measures with independent intelligence reports and fully exploring and reviewing any credible allegations of criminal conduct. • An accurate and up to date register is maintained by the business, of its customers it has rated high risk or identified as PEPs.	**Examples of poor practice:** • The business' procedures are unclear or avoided because a PEP customer is an important business relationship. Follow-up enquiries from monitoring or risk reviews are seen as disadvantageous in order to maintain the relationship. • Enhanced monitoring or the review of high risk customers is not undertaken or has fallen behind schedule due to inadequate resources. • The business dismisses or minimises the importance of information concerning allegations of bribery, corruption or the commencement of criminal proceedings, on the grounds that the customer has not yet been successfully prosecuted in a court of law or that there is a lack of public information to verify the veracity of those allegations. • The business does not maintain a reliable and up to date record of the proportion of high risk rated customers, or those it has identified as PEPs, which make up its overall customer base.

10: RELIANCE ON OTHERS

Self-Assessment Questions:

- What measures have been taken by the business to assess the suitability of those who have certified copies of verification documentation?

- What measures have been taken by the business to prevent reliance upon chains of certified copy documentation? (e.g. where a certifier re-certifies copy documentation without having met the underlying individual or seen the original documents)?

- Does the business currently outsource any functions which form a part of its compliance arrangements? If so, what measures are taken to oversee those functions to verify whether they are being undertaken in compliance with the Regulations and rules in the Handbooks?

- Does the business have a clear understanding as to the proportion of its customer base for which it relies upon Introducers? Is this considered as part of its business risk assessment?

- What measures are taken to obtain assurance that Introducers relied upon by the business have appropriate risk grading procedures, conduct appropriate and effective CDD procedures in respect of its customers, including EDD measures for PEP and high risk rated relationships, throughout the duration of the introduced relationship?

- What measures are taken by the business to ensure that it is kept apprised by its Introducers of any subsequent changes to an introduced customer's risk profile?

- To whom does the business act as an Introducer? Does it maintain a register of the parties for whom it acts in this capacity and the customers involved?

- Does the business have a program of testing to ensure that its Introducers are able to fulfil the requirements of Chapters 4 of the Handbooks?

- How does the business determine that its policies and procedures with respect to certification, outsourcing arrangements and introducers, are, and continue to be appropriate and effective to mitigate the specific financial crime risks to which it may be exposed??

✓

Examples of good practice:

- A procedure is in place, and applied by staff, as to how certifiers should be assessed to determine whether they are suitable. This includes, in some instances, the business making direct contact with the certifier and/ or underlying customer or beneficial owner(s).

- Reliance is only placed on a third party where it qualifies as an introducer relationship pursuant to Regulations 10 and the rules contained in Chapters 4 of the Handbooks.

- The business verifies not only that an Introducer will provide copies of CDD documentation upon request and without delay, but that the Introducer continues to satisfy the criteria stipulated in Regulations 10 and the rules in contained in Chapters 4 of the Handbooks,

- Outsourcing arrangements are overseen and reviewed by the business as part of its overall compliance arrangements, with controls in place to ensure that outsourced functions are undertaken in compliance with the Regulations and the rules in the Handbooks.

- When concerns arise on the reliability of CDD conducted by a particular business Introducer, or a significant number of SARs relate to clients they introduce, consideration is given to terminating the business relationship with the Introducer.

✘

Examples of poor practice:

- Failure by the business to have in place policies, procedures and controls on how to verify the suitability of a certifier, prior to accepting the CDD documentation provided in this format. Contact is only ever made with the customer or underlying beneficial owner(s) through intermediaries or other third parties.

- Reliance is placed on assurances provided by a party who regularly refers customers to the business that they have met and verified and the identity of the customer, with no steps taken to formalize this as an Introducer arrangement.

- The business tests the Introducer arrangements on which it relies, but takes no steps to address those instances, including the termination of those arrangements, where an introducer is unable or unwilling to provide the requested CDD upon request and without delay.

- The business outsources or delegates any of its compliance functions to external parties, including subsidiaries and members of the Group of which it is member, but fails to ensure that this party understands and complies with the CDD requirements of the Regulations and rules in the Handbooks.

- The business allows customers to be introduced to another firm through a chain of one or more introducers, including introducers originating from other jurisdictions and non-Appendix C countries.

11: ONGOING MONITORING & REVIEWS

Self-Assessment Questions:

- What are the measures taken by the business to comply with the Regulations and the Handbooks concerning the ongoing monitoring and customer risk review?
- How does the business verify that its monitoring program (whether automatic, manual or both) and customer risk review process are adequate and effective, given its size, nature and complexity?
- How does the business take account of the confluence or accumulated risk that could arise in relation to the financial crime risks to which its business could be exposed, as part of its monitoring program and customer risk review process?
- How does the business ensure that its monitoring program and customer risk review process are informed by the risk profile information collected about its customers and not just the risk rating it has assigned to those customers?
- Are there monitoring measures and risk review procedures in place for high risk rated customers?
- What procedures are in place to guide staff on the steps that should be taken when monitoring activities "flag" or "alert" changes to a customer's risk profile, including expected transactions and activities? How are these findings fed back into the customer's risk profile and ultimately, the business' own risk assessment?
- What is the process used by the business to determine whether changes to a customer's risk profile or transaction activities are suspicious?
- How are the actions taken recorded and retained for future reference?
- What is the process for changing a customer's risk rating as a result of the findings made as a result of a customer risk review?
- How does the business verify that its staff are applying its monitoring measures and customer review processes in the manner required?
- What measures are undertaken by the business to verify that its monitoring program and customer risk review process are sufficiently resourced?
- Through what means does the business verify that the measures taken to undertake ongoing monitoring and customer risk reviews are, and continue to be, appropriate and effective?

✓

Examples of good practice:

- There is a demonstrable connection between the monitoring program implemented and the business risk assessment.
- The nature of monitoring undertaken reflects the specific financial crime risks to which the business could be exposed.
- The monitoring programme and risk review process are informed by the customer risk assessments and customer risk profile characteristics identified as part of that assessment.
- The monitoring programme and risk review process incorporate both timely periodic and event driven measures, on a risk-basis, to ensure that customers' risk profiles remain up to date and their risk assessments current.
- The business proactively undertakes measures to promptly investigate any changes to risk characteristics and that exiting risk ratings are reviewed to ensure that the appropriate risk rating is assigned.
- The monitoring programme and risk review process are designed to take account of the risk appetite of the business and resourcing required to undertake appropriate investigation and follow-up on monitoring and risk review findings.
- Procedures are designed to ensure that the business is made aware, on a timely basis, of changes in a customer's use of structures and legal arrangements, including changes in beneficial ownership.

✘

Examples of poor practice:

- The business' approach towards monitoring is not informed by the outcome of the business risk assessment, or any subsequent changes made to that assessment.
- The monitoring programme is generic in nature and does not take account of the financial crime risks specific to the business.
- The quality and effectiveness of the monitoring programme and risk review process are compromised by the incomplete nature of customer risk profile information recorded by the business, especially in relation to the customer's expected activity.
- The monitoring programme or risk review process is only applied on a "trigger event" basis.
- Where changes in risk characteristics occur, additional scrutiny of transactions is not undertaken to ensure that they are consistent with the customer's profile, including, their source of funds and source of wealth.
- Monitoring measures and risk reviews are not designed to take account of available resourcing. As a result these measures are not undertaken at all or well after set deadlines.
- Changes to a customer's beneficial ownership are fed back into the assessment process, but it is left to the discretion of front line staff or customer relationship managers to decide whether a change of risk rating is required.

12: REPORTING SUSPICION AND LIAISON WITH LAW ENFORCEMENT

Self-Assessment Questions:

- Does the business ensure that its policies, procedures and controls concerning suspicious activity reporting (SAR) are reviewed by the Board at appropriate intervals?
- Does the business measure the appropriateness and effectiveness of its SAR policies procedures and controls, taking into account the size, nature and complexity of the business?
- Are the reasons relied upon by the MLRO in deciding whether to report a SAR to the FIU documented and retained?
- Through what measures has the business verified that SARs are being promptly considered by the MLRO?
- Are the policies, procedures and controls concerning SAR reporting understood by the staff and senior management of the business?
- Through what measures does the business determine whether its staff are reporting any suspicion to the MLRO? If not, what steps have been taken to determine why reports are not being made?

✓

Examples of good practice:

- SAR policies, procedures and controls are written in a manner so that they can be readily understood by the staff.
- SAR policies, procedures and controls are tailored to the size, nature and complexity of the business.
- There are policies, procedures and controls in place to evidence that the outsourcing service providers of the business are aware of and can report any suspicion to the MLRO.
- The decision making related to SARs is documented, readily accessible and actually applied.
- The MLRO is aware of his obligations to report and understands the process of disclosing suspicious activity and transactions via the Themis system of the FIU.

✗

Examples of poor practice:

- SAR policies, procedures and controls comprise primarily of a summary of the legislative requirements.
- SAR policies, procedures and controls are generic and are not designed with the nature and size of the business, its products and services in mind.
- SAR policies, procedures and controls fail to reference the importance of reporting attempted transactions or rejected business relationships.
- SAR policies procedures and controls are overly complex and end up discouraging reporting by the staff.
- The outsourcing service providers of the business are not made aware of the local reporting requirements for SARs.
- Failure to have a process to facilitate reporting back to the MLRO by outsourcing providers where suspicions are formed arising from the services being performed.
- The MLRO passes all internal reports to the FIU without considering whether they truly are suspicious or SARs are not reported to the FIU in a timely manner due to commercial and/or operational reasons.
- The MLRO does not possess the necessary skills and knowledge to assess SARs which it receives.
- Attempted transactions regarded as suspicious are rejected or new business is declined due to suspicions formed, but the business fails to submit a SAR to its MLRO.
- Staff fail to report suspicions formed while undertaking monitoring activities due to over-reliance upon automated systems to identify such activity.

13: SANCTIONS SCREENING

Self-Assessment Questions:

- How does the business undertake sanctions screening of new business relationships and occasional transactions? What types of lists or data does the business use for screening purposes? (e.g. the Consolidated List referred to in Chapters 12 and 14 of the Handbook, internal watchlists maintained by the business, and/or lists from commercial providers)

- How does the business become aware of changes to the Consolidated List or other sources upon which it relies and what steps are taken when this occurs to ensure that none of its existing customers have been included on these lists? (i.e. Are customers re-screened after each update is issued?)

- How is sanctions screening incorporated into the business' ongoing monitoring and customer risk review processes?

- Is there a clear procedure, communicated to staff on the steps to be taken if it is discovered that an existing customer is a named designated person in accordance with the Terrorist Asset-Freezing (Bailiwick of Guernsey), Law 2011 and or a person or entity subject to a sanction in accordance Section the Al-Qaida (Restrictive Measures) (Guernsey) Ordinance, 2013?

- Through what measures does the business determine whether its sanctions screening processes are appropriate and effective?

✓	✗
Examples of good practice:	**Examples of poor practice:**
• The business has considered the most appropriate method and frequency of screening taking into consideration the size, nature and complexity of its business. • Reliance is only placed on a third parties screening methodology, only after the business has taken steps to satisfy themselves it is appropriate. • Where automated systems are used, the business understands how it is calibrated and resources it accordingly where possible matches are identified. • Screening of the entire customer base is undertaken within a reasonable time following updates to sanction lists. • The business implements risk mitigation measures so as to avoid doing business with countries subject to UN Sanctions and countries identified by FATF as having weak AML/CFT requirements.	• The business has assumed that existing CDD enquiries incorporate appropriate sanctions screening checks, without verifying whether this is the case. • The business places reliance on a third party for sanction screening but has not taken steps to satisfy itself that the screening activity has actually been undertaken, or that the third party will advise the business should any positive matches occur. • Where automated systems are used are purchased "off the shelf"; the business neither enquires into the calibration of the system or considers the possible resourcing needs needed to investigate possible matches. • Screening of customer lists is either a one-off exercise undertaken by the firm or only undertaken on a trigger event basis. • There are no policies and procedures in place to ensure that the sanction screening undertaken utilises the most up-to-date version of the Consolidated List. • As a result of a laissez-faire attitude around sanctions screening, the business fails take adequate measures to mitigate its risk of engaging in business involving Designated Persons or individuals or activities subject of a sanctions.