DEPARTMENT OF COMMERCE & INVESTMENT
CAYMAN ISLANDS GOVERNMENT

# Department of Commerce and Investment

# Business Risk Assessment Guideline for Dealers in Precious Metals & Stones, Real Estate and Property Developer.

September 2019

DEPARTMENT OF
COMMERCE & INVESTMENT
CAYMAN ISLANDS GOVERNMENT

*Version 1*

DEPARTMENT OF COMMERCE & INVESTMENT
CAYMAN ISLANDS GOVERNMENT

# Structure of this guideline

## Contents

DEPARTMENT OF COMMERCE & INVESTMENT
CAYMAN ISLANDS GOVERNMENT

# What is this guideline for?

1. This guideline is designed to help you conduct your money laundering and terrorism financing risk assessment (risk assessment) under the Anti-Money Laundering Regulations[1] ("The Regulations").

2. You understand your business better than anyone else. Identifying and measure the level of risks your business faces from money laundering (ML) and terrorism financing (TF), and developing the appropriate strategies to mitigate and control these risks are best placed with you.

3. Completing a risk assessment (RA) is the first step you must take before developing your AML/CFT programme (programme). The RA involves identifying and assessing the inherent risks your business reasonably expects to face from ML/TF. Once you complete your RA, you are then required to put in place a programme that minimizes or mitigates these risks. Your programme **must** be based on the results RA and your entity risk based approach regime.

4. Your AML/CFT programme should be risk-based in order for it to be effective. Your programme **must** manage and mitigate the ML/TF risks identified by your business. For example, based or your risk assessment you rate the type of client as low risk. Based on the rating you can decide to only conduct simplified due diligence programme that is proportionate to your low risk (see *Part V of the regulations*).

5. Following this guideline is not mandatory. However, you **must** undertake a risk assessment and you **must** establish a programme. (*See regulation 8 of The Regulations*).

6. Your RA and AML/CFT programme should reflect a risk-based approach (RBA) (*See Part III of the regulations)* that allows your business a degree of flexibility in the steps you take when meeting your AML/CFT obligations. Special note should be taken on the fact that a risk-based approach does not prevent you from engaging in transactions/activities or establishing business relationships with customer you have rated as higher-risk. Alternately, your RBA should help you to effectively manage and prioritize your response to those ML/TF risks.

7. All examples in this guideline are only suggestions aimed to help you meet your obligations under the regulations. They are not exhaustive and are highly illustrative in nature.

[1] 2019 (Amendment) & 2018 (Revisions)

8. This guideline is for information purposes only. It cannot be relied on as evidence of complying with the requirements of the Regulations. It does not constitute legal advice from any of the AML/CFT supervisors and cannot be relied upon as such. After reading this guideline, if you still do not understand any of your obligations you should contact your AML/CFT supervisor or seek independent professional advice.

9. You can access the AML/CFT guidance referenced in this guideline at the following website: www.dci.gov.ky

## Terms used in this guideline

10. For the purposes of this guideline, the following definitions apply. These are not defined within the regulations.

- *Material change* – ML/TF risk to your entity is not static and can change quickly. A material change is an event; activity or situation that you identify that could change the level of ML/TF risk you may encounter.

- *Risk-based approach* - refers to the conducting of a risk assessment that's used for the implementation of appropriate AML/CFT measures in response to risks you identified. An effective RBA allows you to exercise informed judgement when making decisions in order to meet your AML/CFT obligations. Under a RBA, there is no "zero risk".

- *Inherent risk* is the assessed ML/TF risk before any AML/CFT controls and measures are in place.

- *Residual risk*- is the assessment of your AML/CFT risk (inherent risk) and how well the controls and measures have been put in place mitigates those risks. Your residual risk reflects the portion of risks that is not mitigated by the controls (the gaps in your controls).

- *Gatekeepers* – Designated non-financial businesses and professions such as real estate, accountants, legal, and trust and corporate service provider sectors are known as "gatekeepers". Gatekeepers denotes to the role they play in providing products and services that can be used to facilitate the entry of illicit funds into the legitimate financial system

DEPARTMENT OF COMMERCE & INVESTMENT
CAYMAN ISLANDS GOVERNMENT

# Part 1: Introduction

## The Anti-Money Laundering Regulation 2018

11. The purposes of the Regulations are to:

- detect and deter money laundering (ML) ,terrorism financing (TF) and proliferation financing (PF);
- maintain and enhance Cayman Islands international reputation by adopting, where appropriate in the Cayman Islands context, recommendations issued by the Financial Action Task Force (FATF);
- contribute to public confidence in the financial system.

## What you have to do

12. As a supervised entity, the first things you should do as part of your obligations under the Regulations are:

- appoint an Anti- Money Laundering Compliance Officer (AMLCO)
- appoint an Anti- Money Laundering Reporting officer(AMLRO)
- conduct a risk assessment to identify and determine the ML/TF risks your business may encounter in the course of your business
- develop and implement a programme containing the procedures, policies and controls used to manage and mitigate those risks and that supports continuous monitoring.

## Risk Assessment (RA)

13. A core element of your AML/CFT regime is an adequate and effective RA reflective of your business. The RA is the base of a balanced risk-based AML/CFT framework. DCI as your AML/CFT supervisor expects that you have a clear understanding of the ML/TF risks and vulnerabilities you face during the course of business.

14. The RA is the foundation document for your entire AML/CFT regime. Therefore you **must** base your policies & procedures on findings detailed within your RA. This should be clearly explained in your RA and documented in AML programme.

## Using AML/CFT guidance

15. You **must** consider any applicable guidance material produced by DCI as your AML/CFT supervisory body, the Cayman Islands Government and any other information provided in relation to the regulations. DCI strongly recommend that you become familiar with the following documents before you undertake your risk assessment.
    - The National Risk Assessment (NRA) Summary Report
    - Sector risk assessments (SRAs) produced by the DCI
    - Industry-specific guidance produced by DCI for Real Estate and Dealers in precious Metals and stones.
    - Guidance Statements published by DCI on regulatory matters
    - The Anti-Money Laundering Regulations
    - Cayman Islands Typologies

## Legal obligations relating to risk assessments

16. As a supervised entity you have a number of obligations under the Regulations in relation to your risk assessment:

    - Your risk assessment **must** identify the risk of ML/TF you may reasonably expect to face in conducting your business.
    - Your risk assessment **must** enable you to determine the level of risk involved in relation to your obligations under the regulations. This includes the ML/TF risk presented by *your customer*, *the products & services, the delivery channels transactions* you offer and the country or *geographic area* in which the customer resides or operates.
    - Your risk assessment **must** be in writing and include a description of how it will be kept up to date.
    - You must implement policies, controls and procedures. These **must** be approved by senior management (if structure permits). It should enable the entity to manage

and mitigate the risks that have been identified by the country or by the relevant financial business.

- You **must** implement mechanisms to monitor the policies, controls and procedures implemented.
- All the relevant risk factors must be considered you before determine what the level of overall risk is and the appropriate level and type of mitigation(s) to be applied.
- You **must** use your risk assessment to develop your programme as set out in the Regulations (*see Part III of the regulations*) for further information.

17. You **must** review your risk assessment to ensure it is up to date, identifies any deficiencies, and make any changes as necessary.

- *You **must** identify and assess the money laundering or terrorist financing risks that may arise - relating to the development of new products (such as virtual currencies), new business practices, including new delivery mechanisms and the use of new or developing technologies for both new and pre-existing product. ( e.g. How you will treat customers that request sale to be conducted using virtual currencies)*
- take enhanced customer due diligence to manage and mitigate the risks where higher risks are identified
- Your risk assessment **must** be independently audited by an appropriately qualified person at your request or at any other time at the request of your AML/CFT supervisor.

18. There is no one size fits all risk assessment, however, the assessment of inherent risk is usually a predominantly quantitative exercise driven by data available in your business. On the other hand the assessment of controls is principally a qualitative judgment based exercise.

19. When evaluating your risk assessment (and your compliance regime), DCI and/or external auditors will want to explore both **adequacy** and **effectiveness of both mechanisms**. Adequacy is described as how compliant your risk assessment is with your obligations of the Regulations. Effectiveness represents how well the practical

application of the risk assessment meets the obligations under the Regulations. This will be represents in DCI supervisory report after on or off site inspection.

# Background

20. Financial Action Task Force (FATF) recommendations - All countries experience illicit international money flows exposure. There is no exemption. FATF based on input from international experts has continuously presented the global nature of ML/TF in their work. The FATF 40 Recommendations and 11 Immediate Outcomes represent the global standard of AML/CFT. It is important that Cayman Islands compliance regulatory regime demonstrates effective use of these standards and part of our international reputation and our ability to combat ML/TF. Cayman Islands were evaluated on these standards and outcomes in 2017.

## Terrorism financing

21. Although TF risk is assessed as medium in Cayman Islands, it is prudent to provide guidance on the vulnerabilities and risks associated with the global issue of TF.

## Stages of money laundering

22. ML is generally considered to take place in three phases: placement, layering and integration. Although these are widely known with the AML/CFT arena, it is worthwhile covering some of the basics of ML/TF before considering ML/TF risk. TF shares many of the characteristics of ML but may also involve legitimate funds and usually involves smaller amounts.

23. **Placement** occurs when criminals introduce proceeds of crime into the financial system. This can be done by breaking up large amounts of cash into smaller sums that are then deposited directly into an account, or by purchasing shares or by loading credit cards. In some offences, such as fraud or tax evasion, placement is likely to occur electronically and may be inherent in the offending.

24. **Layering** occurs once proceeds of crime are in the financial system. It involves a series of changes or movements of funds in order to distance or disguise them from their criminal origin. The funds might be channeled through the purchase and sale of investment instruments or high-value goods i.e. gold, luxury boats, art, vehicles etc. or be wired through various accounts across the world. In some

instances, the launderer might disguise the transfers as payments for goods or services, giving them an appearance of legitimacy.

25. **Integration** occurs once enough layers have been created to hide the criminal origin of funds. This stage is the ultimate objective of laundering: funds re-enter the legitimate economy, such as in real estate, high-value assets, or business ventures, allowing criminals to use the criminal proceeds of offending.

### Predicate offences

26. Predicate offences are the crimes underlying ML/TF activity. Some predicate offences for ML are related to financial crime, the largest category being fraud. It is important that you understand the various types of predicate offences. Please refer to your relevant Industry Guidance Notes for more information on predicate offending.

## Part 2: Identifying Risk

27. As part of assessing risk, you **must** first address your "inherent risks". These are the ML/TF risks that are present before you apply controls and mitigations. You may wish to assess your "residual" risk (the remaining risk after your controls and mitigations are put in place). This is a very important part of your risk assessment. You may compare your residual AML/CFT risk with your overall risk appetite for your business to determine whether you are comfortable with the level of risk that is un-mitigated or whether you need to increase your controls or diminish your exposure to inherent risk in some areas. DCI as your AML/CFT supervisor will expect that your risk assessment deals with inherent risk. If you include residual risk you **must** record how you derive at the rating.

28. When you identify how your business may be vulnerable to ML/TF risks, you **must** consider and document the following ( *see section 8 of the regulations*):

- the nature, size and complexity of your business
- the products and services you offer
- the way you deliver your products and services
- the types of customers you deal with
- the countries you deal with
- the institutions you deal with.

## The nature, size and complexity of your business

29. The nature, size and complexity of your business play an important role in how attractive or susceptible it is for ML/TF. For example, because large businesses are less likely to know their customers personally, they could offer a greater degree of anonymity than a small business. Likewise, a business that conducts complex transactions across international jurisdictions could offer greater opportunities to money launderers than a purely domestic business.

30. Use of company data will help you determine what parts of your business are vulnerable to ML/TF activity. For instance, you may have identified a higher-risk product, but without knowing how many of those products and service you have provided to customers, and where the customers are domiciled, will result in a flawed assessment of risk. Using your corporate data will help in analyzing this potential risk. Effectively this is synonymous with good record keeping practices.

## The products and services your business offers

31. The nature of some products and services makes them vulnerable to ML/TF. When considering whether the products and services your business offers could be exploited for ML/TF purposes, we recommend you consider issues such as:

    - Does your product/service allow for anonymity?
    - Does your product/service disguise or conceal the beneficial owner of your customer?
    - Does your product/service disguise or conceal the source of wealth or funds of your customer?
    - Does your product/service allow payments to third parties?
    - Does your product/service commonly involve receipt or payment in cash?
    - Has your product/service been identified in the NRA, FRA guidance material or SRAs as presenting a higher ML/TF risk?
    - Does your product/service allow for the movement of funds across borders?
    - Does your product or service allow a customer to quickly turn funds (e.g. case of resale of purchased assets or full refund)

32. It is to be noted that several other factors can contribute to the ML/TF risk of your products and services. It is your responsibility to identify those factors as part of your risk assessment. Domestic AML/CFT guidance materials will help you in this exercise. Other documents published in relation to the methods and trends used for ML/TF typologies by the FATF, Caribbean Action Task Force (CFATF), and other overseas AML/CFT agencies can be useful.

## The way your business delivers its products and services

33. The way your business on-boards your customers and delivers your products and services affects its vulnerability to ML/TF. All things being equal, face to face transactions are generally associated with a lower level of risk. For example:

- Does your business have non-face-to-face customers (via post, telephone, and internet or via intermediaries)? What is the volume of that business?
- Do you provide your products/services via the internet?
- Does your business have indirect relationships with customers (via intermediaries, etc.)?
- Do you provide your products/services via agents or intermediaries?
- Do you provide your products/services to overseas jurisdictions?

## The types of customers your business deals with

34. It is understood that some categories of customers pose a higher risk of ML/TF than others, especially when combined with higher-risk products/services and jurisdictions.

35. Part V and VI of the Regulations sets out circumstances where you must conduct simplified customer due diligence (CDD) and enhanced customer due diligence (EDD) where applies respectively.

36. Questions you will need to ask yourself about your customers, new and existing, include:

- Are they a legal arrangement or a legal person?
- Have you identified beneficial ownership?
- Are they specified in the regulations as requiring EDD (e.g. PEPs or when called to do so by the FATF)?

- Are they involved in occasional or one-off activities/transactions above a certain threshold?
- Do they use complex business structures that offer no apparent financial benefits?
- Are any of your customers a politically exposed person (PEP)?
- Are your customers a cash-intensive business?
- Are they involved in businesses associated with high levels of corruption?
- Do they have an unexplained or hard to verify source of wealth and/or source of funds?
- Do they conduct business through, or are they introduced by, gatekeepers such as accountants, lawyers, or other professionals? (Refer to your relevant industry guidance for the relevant gatekeepers.)
- Are any of your customers a non-profit organization?
- Have they been identified in the NRA, typologies, any guidance material or SRAs as presenting a higher ML/TF risk?

37. This list is not exhaustive, and many other factors can contribute to customer ML/TF risk. As with your products and services it will be your responsibility to identify those factors as part of your risk assessment. Domestic and international guidance material will help you in this exercise.

## The countries your business deals with

38. It is critical that you understand that the risks associated with a country are wider than having insufficient AML/CFT measures in place. It is also vital to recognize the international operational nature of ML/TF and that Cayman Islands reputation as a high-integrity, low-corruption jurisdiction makes it vulnerable to abuse. Country risk can result from:

- ineffective AML/CFT measures
- ineffective rule of law and economic instability
- high levels of organized crime
- prevalence of bribery and corruption
- association with TF
- conflict zones and their bordering countries
- production and/or transnational shipment of illicit drugs

39. In determining your country risk, your AML/CFT supervisor (DCI) would have published RE, PD and DPMS Guidance Notes. Other information sources that can help you in assessing country risk include:

- FATF list of high-risk and non-cooperative jurisdictions
- FATF mutual evaluation reports
- European Union AML and tax blacklists
- Basel AML Index
- United Nations Office on Drugs and Crime (UNODC) reports
- Transparency International Corruption Perceptions Index
- trusted and independent media sources.

40. You may want to check if countries are subject to United Nations sanctions, and any other sanctions that may be applicable.

### The institutions your business deals with

41. Some institutions present more ML/TF risk than others. This may be due to the nature of their industry or their association, or the types of business relationships that they have. For instance, financial institutions that are unregulated are more likely to be used for ML/TF purposes or operated by criminals to disguise beneficial ownership.

### Other factors to consider when identifying aspects of your business that may be susceptible to ML/TF

42. The Regulation also sets out special steps you must take in relation to PEPs and new technologies. This information should help you to identify high-risk areas of your business.

43. The summary NRA and SRAs are useful sources of information when identifying how your business could be used for ML/TF. You should also consider emerging trends that are signaled by the FRA in their guidance when identifying risks in your business. Information on current ML/TF methods is available on the CFATF and FATF and DCI websites. This website also has links to other internet pages that you could refer to when assessing the risk your business could be reasonably expected to face.

## Part 3: Assessing risk

44. Risk can be defined in many ways, and there is no one-size-fits-all assessment model for this process. Once you have identified the ML/TF risk that you face during business, you must determine the level of that risk. When assessing risk, you should consider:

- each element of risk you have identified
- your business experience and data in relation to that risk
- information and guidance published by the AML/CFT supervisors and the FRA
- information and guidance published by international organizations such as the FATF, CFATF and UNODC, and other AML agencies from equivalent jurisdictions such as United Kingdom.

45. You should allow for the different situations that currently arise in your business or are likely to arise in the near future. For instance, your risk assessment should consider the impact of new products, services or customer types, as well as new technology. In addition, ML/TF risks will often operate together and represent higher risks in combination.

46. Potential ways to assess risk include but are not limited to:
- how likely is an event to occur
- the potential consequence of that event
- the effect of uncertainty on an event

47. Some examples are provided later in this section, but whichever method you use you will need to explain and demonstrate its adequacy and effectiveness to your AML/CFT supervisor **and** ensure it is appropriate and proportionate to your organizational needs.

48. Your assessment of risk should be informed, logical and clearly recorded. For instance, if you have identified gatekeepers as presenting higher inherent risk in relation to the delivery of your product, your risk assessment should indicate how you arrived at this rating (domestic guidance, case studies, direct experience).

## Risk assessment (lower complexity)

49. In line with the issued AML/CFT supervisor guidance by your DCI, you may want to assess risk by only considering the likelihood of ML/TF activity. This assessment should involve considering each risk factor you have identified, combined with your business experience

and information published by regulators and international organizations such as the FATF. Your likelihood rating could correspond to:

| Very unlikely | Possible | Likely | Very likely |
|---|---|---|---|
| There is very little chance of ML/FT occurring in this area of your business. | There is a small chance of ML/FT occurring in this area of your business | There is a moderate chance of ML/FT occurring in this area of your business. | There is a high chance of ML/FT occurring in this area of your business |

50. For example, you may have identified that one of your products is vulnerable to ML/TF based on ease of access. Your risk assessment highlights the product is easily accessible, that many customers are using it, and it is used in higher-risk jurisdictions. Combined with domestic and international guidance, you assess that the inherent risk rating of this product as likely.

51. Your programme should then address this *likely risk* with appropriate control measures. You will need to do this with each of your identified risks.

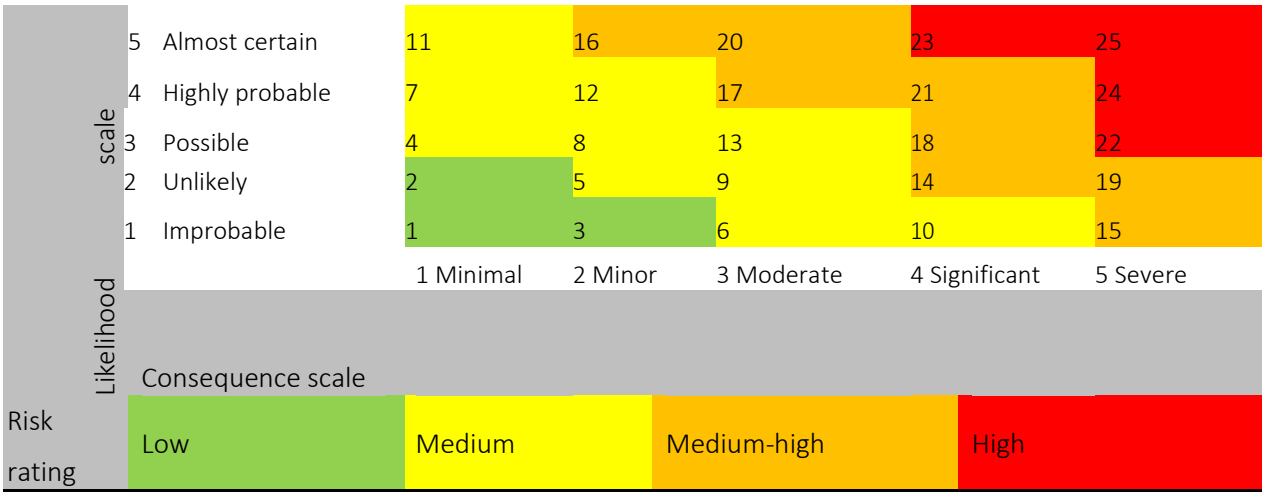
## Risk assessment (medium complexity)

52. Alternately you can determine the level of risk by working out how ***likely*** the risk is going to happen and cross-reference that with the ***consequence*** of that risk (see the example of a risk matrix below).

53. Using likelihood ratings and consequence ratings can provide you with a more comprehensive understanding of your risk and the guide to develop a robust framework to help you arrive at a final risk rating. These ratings will assist you in applying the appropriate risk management measures as detailed in your programme.

54. For example, you may have identified that one of your products is vulnerable to ML/TF and you assess that the likelihood of this product being used in ML/TF activity is *highly probable*. You assess the impact of the identified risk happening in terms of financial loss and assess the consequence as *moderate.*

55. Cross-referencing *highly probable* with *moderate level of impact* in the risk matrix below results in a final inherent risk rating of *medium-high*. Your programme should then address this *medium-high* risk with appropriate control measures. You will need to undertake this exercise with each of your identified risks. The risk matrix below is provided as an illustrative example only.




56. You could assess risk likelihood in terms of threat and vulnerability. For example, you may consider domestic drug trafficking as the threat, and your accounts dealing with cash payments as the vulnerability. Depending on the risk assessment method you use, this could result in an inherent risk rating of *highly probable*. You may then want to assess the impact of this event on your business and the wider environment.

57. Determining the impact of ML/TF activity can be challenging but can also help you focus your AML/CFT resources in a more effective and targeted manner. When determining impact, you may want to consider a number of factors, including:

- nature and size of your business (domestic and international)
- economic impact and financial repercussions
- potential financial and reputational consequences
- terrorism-related impacts
- wider criminal activity and social harm
- political impact
- negative press

58. You may want to give more weight to certain factors to provide a more nuanced understanding of your ML/TF risk.

59. In addition, you may want to consider how your risks can compound across the various risk factors. For example, you may identify that one of your products is high-risk and is being used in a high-risk jurisdiction that is directly involved in the production or

transnational-shipment of illicit drugs. As such, you assess the compounded risk of this scenario as presenting an inherent risk rating of severe. You would be expected to prioritize and allocate your resources accordingly.

# Part 4: Applying a risk assessment

60. Your risk assessment should help you rank and prioritize your risks and provide a framework of how you will manage/mitigate those risks. The AML/CFT controls you apply in each area of your business should be commensurate in nature and severity to the risks you identified, with more compliance resources addressed to areas of higher risk.

61. Your risk assessment **must** enable you to prepare a comprehensive risk based programme. It should enable you to meet your relevant obligations under the Laws and regulations, including your obligations to conduct CDD, ongoing monitoring and report suspicious activity.

64. Your risk assessment should help in determining suspicion and consequently assist in the decision to submit an SAR to the FRA. You **must** submit an SAR to the FRA if you think activities or transactions are suspicious. For instance, you may consider unexpected international activity from a high-risk jurisdiction in relations to your product and services, and submit an SAR.

65. You **must** conduct ongoing CDD. Your risk assessment will help you target and prioritize the resources needed for ongoing CDD. For instance, you may want to undertake ongoing CDD on your high-risk customers on a more regular basis than on your lower-risk customers.

66. You **must** undertake account monitoring. Your risk assessment will help you design the triggers, red flags and scenarios that can form part of your monitoring. For instance, you may want the activity of a high-risk customer in a high-risk jurisdiction (as identified in your risk assessment) to be subject to more frequent and in-depth scrutiny. Increased training in areas shown as high risk in your risk assessment can be used as a mitigation tool.

## New and developing technologies and products

67. New and developing technologies and products can present unknown ML/TF risks and vulnerabilities. In addition, new methods of delivery may be able to bypass existing AML/CFT measures to allow anonymity and disguise beneficial ownership. Your risk assessment should consider whether your business is, or may be, exposed to customers involved in new and developing technologies and products. Your programme should detail

the procedures, policies and controls that you will implement for this type of customer and technology.

### Material changes and risk assessment

68. Your risk assessment should adapt when there is a material change in the nature and purpose of your business or your relationship with a customer. A material change could present an increase, or decrease, in ML/TF risk.

69. Material change could include circumstances where you introduce new products or services or have customers (or their beneficial owner) based in new jurisdictions. Material change can include when you start using new methods of delivering your services or you have new corporate or organizational structures. It could result from you deciding to outsource CDD functions or changing your processes for dealing with PEPs. In these circumstances, you may need to refresh your risk assessment.

## Part 5: Review and audit of risk assessment

### Reviewing a risk assessment

72. You **must** review your risk assessment to:

- ensure it remains current at all times
- identify any deficiencies in its effectiveness
- make any changes that are identified as being necessary in this process.

73. You may want to schedule this annually as part of your annual report process and/or as a result of a trigger event. A trigger event could be the emergence of new technology; a new customer base; new services or products; new ML/TF risks as determined by the FATF, AML/CFT supervisors or the FRA; or updated regulations. Having good version control of documents is useful to demonstrate the effectiveness of framework.

### Auditing a risk assessment

74. You **must** audit your programme (as well as your risk assessment) every two years, or at any other time at the request of your AML/CFT supervisor. You **must** provide a copy of your audit to your AML/CFT supervisor on request.

75. *Independents Audit* – The Regulations states that your risk based programme must include an appropriate effective risk-based independent audit function to ensure that

you continue to review the robustness of your framework and make the necessary changes.

76. The audit must be conducted by an independent person – Your auditor **must** be independent, and not involved in the development of your risk assessment or the establishment, implementation or maintenance of your programme. The person/s appointed to undertake the audit may be a member of your staff (for instance, an internal audit team), provided they are adequately separated from the AML/CFT area of your business. You should be able to justify to your AML/CFT supervisor how your auditor is independent.

77. You may choose to appoint an external firm to undertake both the audit and review provided you are satisfied there are appropriate separation and conflict of interest arrangements. The annual report that you are required to provide to your AML/CFT supervisor **must** consider results and implications of the audit.

# Part 6: List of abbreviations

78. The table is included for reference purpose. It contains abbreviation and acronyms used in this document and the wider AML/CFT environment.

| | |
|---|---|
| AML/CFT | Anti-Money Laundering / Counter Terrorism Financing |
| AMLCO | Anti-Money Laundering Compliance Officer |
| AMLRO | Anti-Money Laundering Reporting Officer |
| CDD | Customer Due Diligence |
| CFATF | Caribbean Financial Action Taskforce |
| DCI | Department of Commerce and Investment |
| EDD | Enhanced Due Diligence |
| FATF | Financial Action Taskforce |
| FRA | Financial Reporting Authority |
| ML | Money Laundering |
| ML/TF | Money Laundering / Terrorism Financing |
| PEPs | Political Exposed Persons |
| PF | Proliferation Financing |
| RA | Risk Assessment |
| SAR | Suspicious Activity Report. |
| UNODC | United Nations Office on Drugs and Crime |