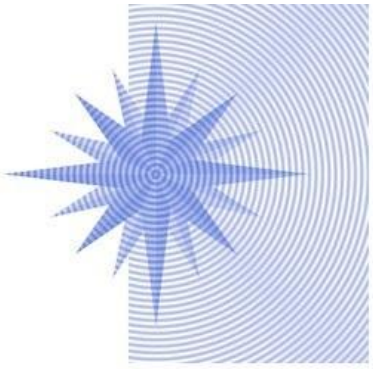


Banco Santander
Bank of America
Bank of Tokyo-Mitsubishi UFJ
Barclays
Citigroup
Credit Suisse
Deutsche Bank
Goldman Sachs
HSBC
J.P. Morgan Chase
Société Générale
Standard Chartered
UBS

the Wolfsberg Group

The Wolfsberg
Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery & Corruption

Financial Crime Risk Assessments are one element of the Financial Crime Compliance (FCC) toolkit available to Financial Institutions/Firms (FIs) which can be used to strengthen a FI's compliance framework. The assessments highlight key risk areas, how well those risks are managed and support a risk-based allocation of resource to the highest risk areas, as well as the establishment of strategic (more long term) and tactical (immediate workaround) action plans for managing the identified risks.

Numerous questions arise as a result of any risk assessment and this document poses some of the more frequent ones, as well as providing some guidance as to how to address them. Other departments across a FI, including business risk management, compliance monitoring or audit may also undertake forms of risk assessment and therefore both the undertaking and the results of all risk assessments should be coordinated, to the extent that this is possible.

The Wolfsberg Group of International Financial Institutions[1] has prepared these FAQs, based on the Wolfsberg Group's views on current best practices and, in some aspects, on how the Group believes those practices should develop over time. The Group believes that these FAQs will contribute to the promotion of effective risk management and further the goal of Wolfsberg Group members to endeavour to prevent the use of their institutions for criminal purposes.

A Glossary of key terms referred to in these FAQs is included in **Appendix A**.

[1] The Wolfsberg Group consists of the following financial institutions: Banco Santander, Bank of America, Bank of Tokyo-Mitsubishi-UFJ Ltd, Barclays, Citigroup, Credit Suisse, Deutsche Bank, Goldman Sachs, HSBC, JPMorgan Chase, Société Générale, Standard Chartered and UBS. These FAQs also benefited from the contributions of American Express, Lloyds and RBS for which the Wolfsberg Group members are grateful.

Preamble

The literature of how people view risk depending on context, group size and numerous other factors is extensive. Most FIs will be used to assessing risk in areas such as Credit Risk or Market Risk, where risk can be easily quantified and is usually assessed prior to accepting that risk. Financial Crime Risk Assessment, however, differs somewhat, focusing on assessing 'consequential' risk, i.e. risk that is reflective of a FIs internal and external environment, including mitigating controls. For both types of assessment, however, quantitative and qualitative risk assessment methodologies have proven to be useful in helping FIs assess risks, understand observed phenomena, explore the sources and impacts of financial crime risk and develop tools and methods for managing those risks. At their best, they remove a great deal of bias and subjectivity from risk analysis, as well as giving FIs a risk measurement tool.

In January 2014, the Basel Committee on Banking Supervision (BCBS) issued a document, entitled "Sound Management of Risks related to Money Laundering and Financing of Terrorism"[2] which includes the following statement on the importance and conduct of Risk Assessments:

> *"Sound risk management requires the identification and analysis of ML/FT risks present within the bank and the design and effective implementation of policies and procedures that are commensurate with the identified risks. In conducting a comprehensive risk assessment to evaluate ML/FT risks, a bank should consider all the relevant inherent and residual risk factors at the country, sectoral, bank and business relationship level, among others, in order to determine its risk profile and the appropriate level of mitigation to be applied."*

While the BCBS Paper is relatively recent, risk assessments have long been an expectation under other regulatory regimes. In the United States, for example, guidance is provided in the Federal Financial Institutions Examination Council ("FFIEC") Bank Secrecy Act/Anti-Money Laundering (AML) Examination Manual, where it is stated that management should:

> "…structure the bank's BSA/AML compliance program to adequately address its risk profile, as identified by the risk assessment… develop the appropriate policies, procedures, and processes to monitor and control BSA/ML risks. For example, the bank's monitoring systems to identify, research and report suspicious activity should be risk-based, with particular emphasis on higher-risk products, services, clients, entities, and geographic locations as identified by the bank's… risk assessment."[3]

In the UK, The Joint Money Laundering Steering Group Guidance Notes outline some of the considerations that should be taken into account when conducting a risk assessment, the application of a risk based approach being a core theme.[4]

For the purposes of this document, when a Money Laundering (ML) risk assessment is referred to, it is generally understood to include Terrorist Financing, Sanctions and Bribery & Corruption. However, as set forth in question 5 below, while there can be significant commonality in the factors used to conduct ML and Bribery and Corruption (B&C) risk assessments, a B&C risk assessment can also involve additional components which are not typically used in pure ML and sanctions risk assessments. Ultimately, though, how a firm designs its assessment methodology will very much depend on the complexity of the organisation, its footprint and its business focus.

While the approach outlined above is commonly employed by many FIs, other approaches and variations have been, and will continue to be, leveraged by FIs, such as using risk scenarios, which

[2] http://www.bis.org/publ/bcbs275.pdf
[3] https://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2014.pdf
[4] http://www.jmlsg.org.uk/industry-guidance/article/jmlsg-guidance-current

assess the likelihood and impact of money laundering/terrorist financing scenarios occurring as a way of calculating a FI's inherent risk.

There are many ways to conduct a risk assessment and each FI should implement appropriate methodologies based on a number of different factors, including its size, global footprint, markets, organisation and risk appetite, amongst others. In order for a risk assessment to be successful, senior management, along with key stakeholders, should provide appropriate support to the effort in the context of fostering a robust culture of compliance.

1. What is the purpose of a risk assessment?

The key purpose of a money laundering risk assessment is to drive improvements in financial crime risk management through identifying the general and specific money laundering risks a FI is facing, determining how these risks are mitigated by a firm's AML programme controls and establishing the residual risk that remains for the FI.

The results of a risk assessment can be used for a variety of reasons, including to:

- identify gaps or opportunities for improvement in AML policies, procedures and processes
- make informed decisions about risk appetite and implementation of control efforts, allocation of resources, technology spend
- assist management in understanding how the structure of a business unit or business line's AML compliance programme aligns with its risk profile
- develop risk mitigation strategies including applicable internal controls and therefore lower a business unit or business line's residual risk exposure
- ensure senior management are made aware of the key risks, control gaps and remediation efforts
- assist senior management with strategic decisions in relation to commercial exits and disposals
- ensure regulators are made aware of the key risks, control gaps and remediation efforts across the FI
- assist management in ensuring that resources and priorities are aligned with its risks.

2. How often should an enterprise-wide risk assessment take place?

Undertaking an enterprise-wide risk assessment is a complex and resource-intensive task but nonetheless a necessary one in order to understand a FI's risk environment. The periodicity of the enterprise-wide risk assessment will depend upon a number of factors including the methodology employed, the type and extent of interim validation/verification that is undertaken, the results of the risk assessment, as well as internal or external risk events.

FIs should decide on the appropriate frequency of the risk assessment in order to maintain the relevance of their findings and risk mitigation programme. Some FIs will refresh their risk assessments annually, however, if there are no material changes to the risk environment, some may choose to undertake their risk assessments less frequently. In exceptional circumstances, such as regulatory intervention for example, a risk assessment may be conducted more frequently than annually.

Regardless of the frequency with which an enterprise-wide risk assessment is undertaken, FIs are usually required to report annually on the status of the money laundering risk environment. This can take the form of an Annual Report or other types of reports. As such, one approach is to undertake a trigger-based interim validation of the most recent risk assessment, looking to highlight whether there has been any change to the previously identified risk environment. These changes could stem from internal (e.g. significant increase in suspicious activity reports) or external (e.g. significant enforcement

action against a peer institution) drivers. Any changes may result in the initiation of additional action plans or highlight a need to undertake a more in-depth assessment in certain areas.

Additionally, ad hoc risk assessments may be performed, focusing on higher risk areas and the specific controls that have been implemented to address the given risk. The results from these ad hoc risk assessments can then be incorporated into the next regular ML risk assessment.

FIs should review their methodology on a regular basis (most likely annually) to ensure that any changes in internal or external factors are incorporated appropriately in order to arrive at the most accurate picture of risk possible. Any changes in the methodology employed from one year to the next will need to be clearly documented and approved by the relevant governance function (e.g. senior management, Financial Crime Executive Committee). Changes will need to be assessed in terms of a FI's ability to compare results year on year, otherwise potentially significant changes in the results may not be justifiable, clearly explained or understood. FIs may also choose to have their methodology reviewed regularly by an independent testing function, e.g. audit or an independent third party. This should allow for consistency of risk management within the FI as well as provide a view of how the methodology compares across the industry.

3. How should a risk assessment be organised?

Whichever approach is chosen, FIs should ensure that their approach is clearly documented and approved by senior management. The methodology for the risk assessment must be clearly articulated, especially with regard to the factors being assessed, the criteria used to score, the requisite weightings used in the scoring methodologies, any scoring overrides applied, including the rationale for them and any business line/business unit specific parameters, amongst others. While arbitrary scoring overrides may not be the norm, there may be instances where a manual override is necessary, especially in the first few times a risk assessment is conducted and until such a time as the methodology employed stabilises.

The decision as to who owns and manages the risk assessment may be impacted by how the risk assessment is conducted, i.e. whether by business lines, country, region or enterprise-wide and the decision will be influenced by the structure, global footprint and complexity of a FI. For enterprise-wide risk assessments, a number of risk assessments may be aggregated to a single level to become enterprise-wide, although tactical actions may be owned at a business line level rather than at a FI-wide/Group level. Strategic actions are likely to be owned and driven at a Group or regional level. The owners of actions may differ according to the size and complexity of the FI but should be those individuals who are best positioned to have accountability for ensuring the action can be completed.

The scope of a risk assessment should be clearly articulated, i.e. whether it is a risk assessment that is independent from the business and conducted by compliance, or whether it is an integrated risk assessment, capturing issues identified by both the business and compliance.

Similarly, the form of assessment undertaken, or the types of questions posed, may differ depending on which business area is being assessed and if a FI only covers one or another business area. A FI offering solely wealth management services, for example, may choose to focus its questions and control framework more on geography and client risk, rather than product or delivery channel risk, which could arguably be more of interest to a retail focused business. This would allow a greater level of focus and analysis to be applied to the area that is being assessed.

When undertaking a risk assessment FIs should choose an appropriate format to collate the risk assessment. Available options include the creation of a bespoke internal system to log risk assessment answers and generate risk ratings, the use of electronic spreadsheet programmes, the manual calculation of risk ratings, as well as other potential options. The chosen approach should be

appropriate for the size and complexity of the FI as this could have an impact on the efficiency and manageability of the risk assessment. A FI should investigate which approach is most appropriate and document the rationale behind the decision. When making this decision, a FI should also take into account whether the approach is able to generate risk ratings and track actions that arise through the course of the risk assessment. While actions may be located in a different internal system, it should be recorded that the action arose as a result of the risk assessment.

If using different approaches within a FI, the principles of the risk assessment methodology should be followed consistently so that the relative outputs can be compared in terms of the magnitude of the risks identified. Once a risk assessment methodology has been designed, it would benefit the FI if there is consistency within the methodology at a certain level: i.e. any changes made to the methodology should still allow comparisons to be made to previous risk assessment results, so as to show meaningful increases/stability/decreases in risk across any given FI. An example process for how to structure a risk assessment is given in **Appendix B**.

4. Whose responsibility is it to undertake a risk assessment?

Senior management of a FI are the overall owners of the risk environment. They may delegate the assessment of risk to the Legal/Financial Crime Compliance/AML Unit (AML Unit), which may have primary responsibility for the initiation and delivery aspects of the ML Risk Assessment. This would include tasks such as methodology development, maintenance, periodic refresh process/activity initiation and record keeping of completed assessments. Business line heads, as well as other departments, such as Information Technology, Operational Risk and Payments, for example, may also be required to contribute. It is to be noted that, while the FI's senior management may delegate the risk assessment process to the AML Unit, the ownership of the risks remains firmly with the business, who may also be responsible for carrying out any actions resulting from the gaps or deficiencies identified by the risk assessment exercise (see question 3 above).

The purpose of the risk assessment and the contribution required from each party should be clearly outlined, with FIs considering whether to include specific responsibility for contribution to, and the execution of, the risk assessment as part of the annual objective setting process for relevant staff. FIs should also ensure that timely and appropriate training/guidance is provided to staff involved in the completion of the risk assessment to ensure that a consistent approach is taken, e.g. in relation to the meaning of specific terminology.

The chosen risk assessment framework should be fully endorsed by senior management of a FI and used as one of the tools through which a culture of compliance can be driven. The AML Unit should ensure there are adequate resources allocated to managing the risk assessment process and its outcomes.

5. Should the scope of a ML risk assessment encompass Bribery & Corruption along with other notable financial crimes?

AML Compliance Units at most FIs will manage AML (including CTF), Sanctions and AB&C within a single department, usually the Financial Crime Compliance department. Before initiating a ML risk assessment, a FI should first evaluate and determine what the full scope of the risk assessment will be. Historically, ML risk assessments have focused on client, transaction and other risks associated with more traditional forms of money laundering. However, over time, additional financial crimes have become predicate offences to money laundering, and the breadth of AML compliance has similarly expanded to encompass a greater array of suspicious activities. Therefore, a risk assessment process may involve an evaluation of multiple, and sometimes disparate, activities, including money laundering, international sanctions, bribery and corruption, fraud of various kinds, insider trading and market

manipulation, tax evasion, amongst others. While there can be overlap across the factors used to assess different risks, the factors can also differ substantially in some cases.

FIs may therefore choose to cover all these areas within a single risk assessment, through separate assessment processes, or a combination thereof. Below are issues to consider when determining the scope of a risk assessment:

- Sanctions: A sanctions risk assessment has, to some degree, the most overlap with ML and is often performed in conjunction with a ML risk assessment, but also requires Sanctions-specific, and often only centrally available, data and information feeds. Guidance issued by regulators, particularly in the U.S., sets forth various higher risk factors that should be considered in a sanctions risk assessment, including, amongst other things, international funds transfers; so called, 'non-resident alien accounts', or 'non-domiciled individual accounts'; foreign client accounts; cross-border automated clearing house (ACH) transactions; commercial letters of credit and other trade finance products; transactional electronic banking; foreign correspondent bank accounts; payable through accounts; international private banking; overseas branches or subsidiaries; investments in foreign securities; omnibus accounts / use of intermediaries and third-party introduced business. Many of these, and other similar factors, are traditionally associated with ML risk assessments as well. However, the nature and effectiveness of certain mitigating controls related to sanctions, particularly sanctions screening of payments, receipts, and other asset transfers, may differ from core AML mitigating controls. Other controls, such as the level of due diligence performed on clients at higher risk for sanctions prohibitions will typically be components of a FI's AML programme.

- Bribery & Corruption: Factors used to assess ML risk may also be relevant for assessing B&C risk. For example, the jurisdiction of a FI's clients and/or business units is relevant for both ML and B&C risk. Jurisdictional risk is in part dependent on the existence of relevant laws and regulations, the strength of the regulatory environment and cultural norms, amongst other factors. These factors significantly impact both ML and B&C risk. Certain aspects of a FI's client base will also be relevant for both ML and B&C risk. For example, the volume, percentage and/or size of government-related clients may impact both ML and B&C risk, although to varying degrees. While there is some overlap of factors relevant for assessing ML and B&C risk, certain other factors may be much more relevant for a B&C risk assessment. These may include third parties who act on a FI's behalf, hiring practices, charitable giving and business gifts and entertainment. These, and other legitimate business practices, can potentially be used inappropriately to bestow a benefit on (or receive a benefit from) an individual government official or employee of a client or other third party and, therefore, could pose bribery risks. The propensity and scale of such practices, therefore, should be considered in a B&C risk assessment.

It should be possible to segregate any of these risk types within a risk assessment based on the underlying data that has been collected. This will allow specific views of risk to be presented.

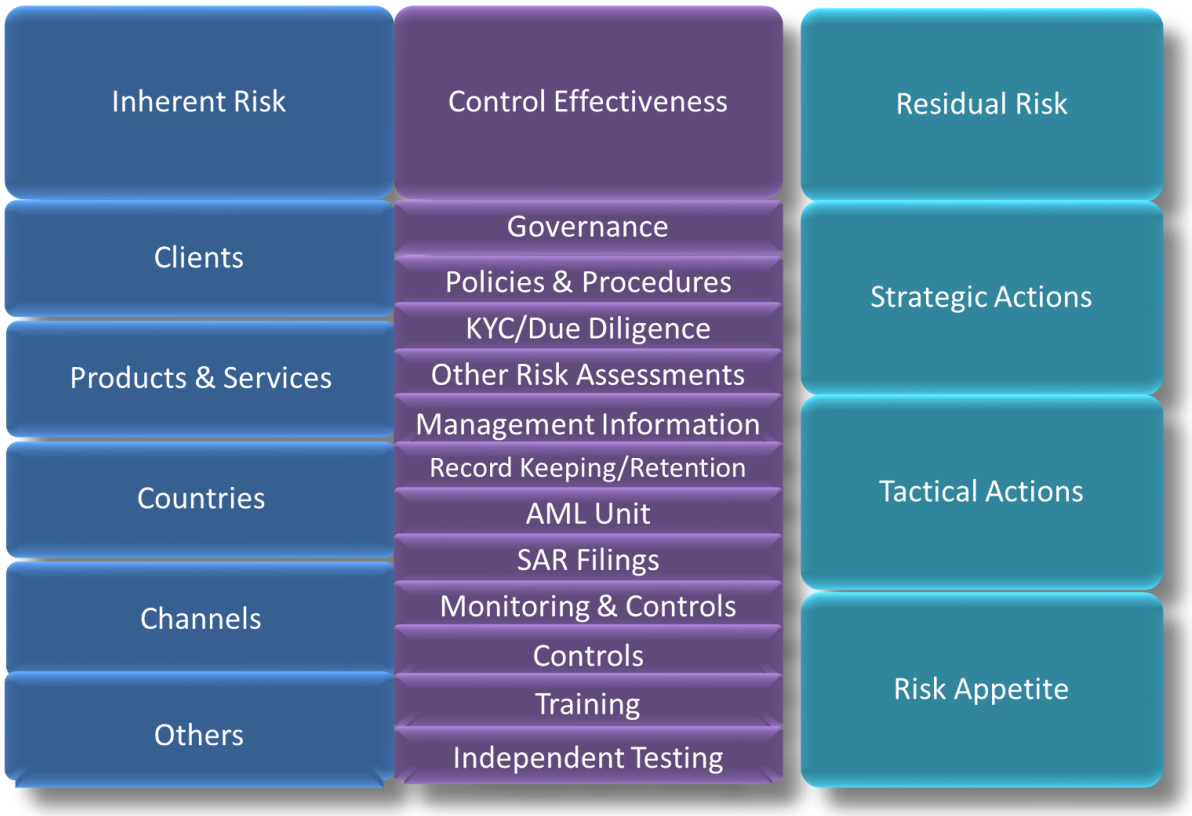
Regardless of whether a FI formally evaluates the above (and other) financial crime risks through the ML risk assessment or through separate assessment processes, it is incumbent on the FI's AML Unit to understand the extent of the risks posed across the FI. Similarly, the AML Unit should understand the effectiveness and deficiencies of the FI's corresponding mitigating controls, irrespective of whether the AML Unit owns the management and maintenance of those controls.

More recently, crimes such as insider dealing and market manipulation have become predicate offences to money laundering and, as such, could be considered in the context of a ML risk assessment. For the time being, however, these are generally considered separately from a ML risk assessment although the methodology used to assess the risks presented is similar. If a new predicate offence is added by a

regulatory body/legislative pronouncement, this may give rise to a review of the methodology to ensure it is appropriately inclusive.

6. What is the conventional/standard ML risk Assessment methodology?

While there are numerous ways to conduct Risk Assessments, increasingly the most common approach used by FIs can be described as the "conventional/standard methodology." The following diagram illustrates what might be expected in practice, although this may clearly vary from one FI to another:



The risk assessment should cover the entirety of the FI's business, though may be conducted in parts, or as part of a rolling cycle, to focus on separate areas, such as divisions, units or specific business lines, countries and/or legal entities. The risk assessment should consider all relevant inherent money laundering risk factors in order to determine its risk profile and in turn assess the nature of mitigating controls, both from a design and operating effectiveness standpoint, in order to arrive at the residual risk, which should be within the FI's established risk appetite. While the risk assessment is the responsibility of the FI as a whole, the money laundering risk assessment will usually be designed and carried out by the competent AML Unit, applying specialist knowledge and expertise alongside the gathering of relevant external and internal information. The risk assessment process can be considered in 3 Phases:

Phase 1:	Determine the Inherent Risk;
Phase 2:	Assess the Internal Control Environment (both design and operating effectiveness); and
Phase 3	Derive the Residual Risk.

6.1 Phase 1 – Inherent Risk Assessment

Inherent Risk represents the exposure to money laundering, sanctions or bribery and corruption risk in the absence of any control environment being applied.

As no two FIs are the same, inherent risk ratings may vary for FIs depending upon the size and scope of their businesses and the risks involved. In order to identify a FI's inherent risks, assessment across the following five risk categories is commonly undertaken, although other factors may also be considered:

1. Clients
2. Products and Services
3. Channels
4. Geographies
5. Other Qualitative Risk Factors

The categories of risk faced by an organisation can be very broad. These broad risk categories are then sub-divided into inherent risk factors that are derived from regulatory guidance or expectations as well as leading industry practices, and include a mix of both qualitative and quantitative criteria. Risk factors are the underlying causes or circumstances where a FI may be used for purposes connected to financial crime.

Managing the risk factors inadequately could lead to reputation risk, regulatory or legal sanction and possible consequent financial costs. Due to the nature of the particular business unit or business line's products and services and client base, a risk based approach is used to determine inherent risk. Each risk factor is usually assigned a score or weighting which reflects the level of risk associated with that risk factor and the prevalence of that risk compared to other risk factors.

FIs should decide what rating should be applied in instances where data, as defined by the methodology, cannot be easily sourced (for example, answering "unknown" to certain questions may result in an automatic high risk/deficient rating) and also consider remedial action required to obtain the data.

6.1.1. Clients

For the purposes of assessing the inherent money laundering risk of a business division, unit or business line, the client base and business relationship should be assessed. A number of Client types, industries, activities, professions and businesses, alongside other factors, such as the length of a client relationship, can increase or decrease money laundering risks. The following categories can be used to stratify the client base and to identify aspects of client risk: client type, ownership, industry, activity, profession and/or business. Some, or all, of these categories may be relevant depending upon the particular division, unit or business line under review.[5]

Each Client type is assigned a risk score, depending upon the expected amount of ML risk each type carries. For the business division, unit or business line in question, the volume (#) of clients that fall within each client type should then be determined/estimated. This data can be utilised to determine what percentage (%) of each business division, unit or business line client types are rated according to the risk classification, e.g. low risk versus moderate, versus high versus higher risk, in order to determine the overall inherent client risk. A FI's approach to categorising risk should be clearly documented. A table of inherent risk score examples for different client types is set out in **Appendix C**.

6.1.2. Products and Services

Alongside "Clients" one of the other major risk components can be found when considering Products and Services Risks, where a FI will seek to identify its portfolio of main products/account types and

[5] It is generally accepted that most FIs will undertake risk assessment across their client base. However, others may choose to undertake risk assessment with greater focus on accounts/transactions. The approach chosen for a FI should be clearly documented and accompanied by an appropriate rationale.

assign an inherent score (for example, low, moderate, high or higher) to each, based on its general inherent characteristics and the degree of money laundering risk present. For the business division, unit or business line in question, the volume (#) of products/account types offered by the business, and (if available), associated account balances or, where relevant, turnover, should then be determined/estimated. This data can be utilised to determine what percentage (%) of each business division, unit or business line products/account types are rated according to the risk classification e.g. low risk versus moderate, versus high versus higher risk, in order to determine the overall inherent product risk. An example table of inherent increased risk scores for different Product/Services and Transactions is set out in **Appendix D**.

6.1.3. Channels

Some delivery channels/servicing methods can increase money laundering risk because they increase the risk that the division, unit or business line does not truly know or understand the identity and activities of the Client. Consequently it should be assessed whether, and to what extent, the method of account origination or account servicing, such as non face-to-face account opening or the involvement of third parties, including intermediaries, could increase the inherent money laundering risk. It should be noted that these accounts may not always lead to an increase in the inherent money laundering risk, e.g. where the Client is known to the FI though undertake their business activity non face-to-face. Non-regulated Clients, or those that are not well known to a FI, are much more likely to present a higher inherent risk of money laundering.

For this risk category the business division, unit or business line will then determine/estimate the percentage (%) of accounts or clients that are rated according to the risk classification e.g. low risk versus moderate, versus high versus higher risk, in order to determine the overall inherent channels risk. An example table of inherent risk scores for different Channel risk factors is set out in **Appendix E**.

6.1.4. Geography/Country

Identifying geographic locations that may pose a higher risk is a core component of any inherent risk assessment and the business division, unit or business line will seek to understand and evaluate the specific risks associated with doing business in, opening and servicing accounts, offering products and services and/or facilitating transactions involving certain geographic locations.

The Geography/Country risk may also be analysed with respect to the location of the business division, unit or business line, and may also include its subsidiaries, affiliates and offices, both internationally and domestically. The aim is to identify the geographic footprint of a FI. For clients, the aim is to identify the number (#) of its clients within each country. The FI will need to decide whether this number should be based on all or some of the following: domicile, incorporation, nationality. In order to map geographies/countries into different risk ratings, a FI's own country risk model or equivalent (appropriately reviewed) third party vendor product may be used. An example table of inherent risk scores for different Geography/Country risk factors is set out in **Appendix F**.

Geography/Country risk may also be considered together with some of the other risk factors in other risk categories, for example, in Clients for FIs, and in Products and Services for Transactions. For example, the percentage of a business division, unit or business line's transactions with a high risk country may provide an indication of the inherent risk from a Geography/Country perspective.

Geography/Country risk will be important in any Sanctions Risk Assessment, not only with respect to sanctioned countries themselves, but also those which may have well known/important links or other significant connections to sanctioned countries. These could include countries bordering, or in close proximity to, sanctioned countries, or those countries which present potential opportunities for the diversion of funds with the intent to violate or circumvent sanctions regulations.

Additionally, Geography/Country risk will also be applicable in any Anti-Bribery and Corruption Risk Assessment. Certain jurisdictions carry increased levels of bribery and corruption risk, usually to do with how those in power are able to abuse their positions for their own financial gain. Where such jurisdictions are present in a FI, the bribery and corruption risks need to be appropriately reflected.

6.1.5. Other Qualitative Risk Factors

Additional risk factors can have an impact on operational risks and contribute to an increasing or decreasing likelihood of breakdowns in key AML controls. Qualitative risk factors directly or indirectly affect inherent risk factors. For example, significant strategy and operational changes, such as the introduction of a major new product, or service, a merger or an acquisition, opening in a new location or closing an entity may affect the inherent risk. These changes may well require a review of existing, or the establishment of new, internal controls, and given that these controls may take some time to become effective, the division, unit or business line will need to assess whether the inherent risk may have temporarily increased or changed. The main "Other Qualitative Risk Factors" might include:

- ***Client base stability***
- ***Integration of IT systems***
- ***Expected account/client growth***
- ***Expected revenue growth***
- ***Recent AML Compliance employee turnover***
- ***Reliance on third party providers***
- ***Recent/planned introductions of new products and/or services***
- ***Recent/planned acquisitions***
- ***Recent projects and initiatives related to AML Compliance matters (e.g. remediation, elimination of backlogs, off-shoring)***
- ***Recent relevant enforcement actions***
- ***National Risk Assessments***

Example tables of potential inherent risk scores for different Other Qualitative risk factors are set out in **Appendix G**.

6.1.6. Is there a common standard for Industry Inherent Risk Ratings?

While business divisions, units and/or business lines' inherent risks can be ascertained by the application and aggregation of risks relating to Client, Products and Services, Channels, Geography/Country and other Qualitative Risk Factors, in many cases, unless unusual or specific additional risks are presented, it is likely that certain parts of a FI will drive a lower rating than others, and alternatively, others a higher rating.

While generic or relative ratings for banking businesses are useful, they should not be used on their own in the absence of inherent risk assessments. For an example of generic inherent risk ratings for the most important banking businesses, see **Appendix H**.

6.2 Phase 2 – Assessment of Internal Controls

Once the inherent risks have been identified and assessed, internal controls must be evaluated to determine how effectively they offset the overall risks. Controls are programmes, policies or activities put in place by the FI to protect against the materialisation of a ML risk, or to ensure that potential risks are promptly identified. Controls are also used to maintain compliance with regulations governing an organisation’s activities. Many of the same controls apply to various activities undertaken within the FI

and will be executed by both the Front Office (1st line) and Compliance (2nd line).[6] The controls in place are evaluated for their effectiveness in mitigating the inherent money laundering risk and to determine the residual risk rating. AML controls are usually assessed across the following control categories:

- ***AML Corporate Governance; Management Oversight and Accountability***
- ***Policies and Procedures***
- ***Know Your Client ("KYC"); Client Due Diligence ("CDD"); Enhanced Due Diligence ("EDD")***
- ***Previous Other Risk Assessments (local and enterprise-wide)***
- ***Management Information/Reporting***
- ***Record Keeping and Retention***
- ***Designated AML Compliance Officer/Unit***
- ***Detection and SAR filing***
- ***Monitoring and Controls***
- ***Training***
- ***Independent Testing and Oversight (including recent Internal Audit or Other Material Findings)***
- ***Other Controls/Others***

Each area is assessed for overall design and operating effectiveness. There may be both a positive or negative indicator of control execution and these should be clearly documented in order to assess the operating effectiveness of each control. Additionally, controls should be linked to Key Performance Indicators or other metrics where possible.

One way in which control effectiveness may be assessed is by undertaking a focused self-assessment by business unit/business line. A self-assessment of this kind can be challenged independently using subject matter expertise as well as existing internal information, such as business risk reviews, audit testing and assurance testing. A specific control may be rated according to a pre-defined rating scale or based on qualitative factors, e.g. 'satisfactory', 'needs improvement' or 'deficient' for each of the above control factors.

For example, for Training, there will be a number of elements required to be present within an effective training framework. As such, the control assessment will focus on each of these elements, such as whether staff training needs have been assessed, whether specialist training is provided for key roles or whether training is being completed on time, requiring the FI to assess whether each element operates satisfactorily, needs improvement or is deficient. For each of these ratings, guidance may be produced for each element under the Training section. This may also be accompanied by an overall rating for the Training section. If providing overall ratings for the section, these ratings should be reflective of the underlying ratings within that section.

If controls are highlighted as either not designed or operating effectively or do not exist, it would be appropriate to raise an action to remedy this if an action is not already underway. In the training example, this could involve the implementation of a revised, targeted training programme for staff, or the establishment of an enhanced due diligence procedure. If an action is already underway, this should be noted when commenting on the deficiency. However, an action should not affect the Residual Risk, i.e. an action is not in itself a mitigating factor to an inherent risk position. The assessment of Inherent Risk and Internal Controls are a 'point in time' assessment and the effective execution of a corrective action will only seek to improve the Residual Risk in the following risk assessment that is conducted.

[6] First and Second Line activities refer to the classic « Three Lines of Defence » Framework where the business is the First Line, Compliance and other Control Functions the Second Line and Audit the Third Line.

As with inherent risk factors above, the response to each area under examination is assigned a score, which, when aggregated, reflects the relative strength of that control. Each area can then be assigned a weighting based on the importance that the institution places on that control. For example, it may be expected that Client Due Diligence carries a larger weighting than Record Keeping and Retention within the risk assessment. An example can be found in **Appendix I**.

6.2.1 AML Unit Override

Risk assessment methodologies should continue to evolve, so as to correspond ever more closely with a FI's view of risk. After completing the assessment of the risk and control categories, the AML Unit (or other functions as determined by the FI) should conduct a data quality review and it may be appropriate in certain circumstances to consider whether to override the inherent risk rating or the control effectiveness rating of any factor or category. While it is easier to justify an increase in the inherent risk rating and/or a decrease in the control effectiveness rating, the reverse should also be possible, although in either case the methodology may need to be reviewed if the changes are very significant.

Some FIs may consider applying an override after calculating the Residual Risk. In all cases, the rationale behind such an override must be thoroughly documented, supported and approved by someone with appropriate authority. In addition to providing for Inherent Risk scores, or Control Environment scores, trend indicators for risk can also be used, such as a scale of increasing, stable and decreasing risk. The need for an override could be indicative of a weakness in the risk assessment methodology and should be reviewed by a FI ahead of the next rollout of the risk assessment.

6.3. Phase 3 – Arriving at the Residual Risk

Once both the inherent risk and the effectiveness of the internal control environment have been considered, the residual risk can be determined. Residual risk is the risk that remains after controls are applied to the inherent risk. It is determined by balancing the level of inherent risk with the overall strength of the risk management activities/controls. The residual risk rating is used to indicate whether the ML risks within the FI are being adequately managed.

It is possible to apply a 3 tier rating scale, to evaluate the Residual Risk on a scale of High, Moderate and Low. Any rating scale could also be used, for example a 5 point scale of Low, Low to Moderate, Moderate, Moderate to High, and High. The following definitions could be considered to describe the level of residual risk applied to a 3 tier rating scale:

i) Low Residual Risk: The overall inherent risk of the FI/business unit/business Line, based on the clients, products/services, channels, geographies and other qualitative factors, is low-to-moderate and the mitigating controls are sufficient to manage this inherent risk;

ii) Moderate Residual Risk: The overall inherent risk of the FI/business unit/business line, based on the clients, products/services, channels, geographies and other qualitative factors, is low-to-moderate and the mitigating controls are not adequate to manage this level of risk, OR the overall inherent risk of the FI, based on the clients, products/services, channels, geographies and other qualitative factors, is high and the mitigating controls are adequate to manage this inherent risk

iii) High Residual Risk: The overall inherent risk of the FI/business unit/business line, based on the clients, products/services, channels, geographies and other qualitative factors, is moderate-to-high and the mitigating controls are not sufficient to manage this inherent risk.

For an example of how a scoring methodology can be configured, see **Appendix J**.

Given the above methodology, certain rules can be adopted within a ML risk assessment when finalising risk ratings, for example:

i) A Strong control environment can lower the residual ML risk in comparison to the inherent risk;

ii) If the FI/business unit/business line receives a High rating of inherent ML risk, it can never achieve a residual ML risk rating of Low; and

iii) In order to improve its residual ML risk, either the inherent ML risk can be reduced or the AML controls can be strengthened.

6.3.1 Weighting and Scoring

Due to the nature of each Business Division's unique business activities, products and services (including transactions), client base and geographic footprint, a risk based approach is used to calculate inherent risk. Each risk factor is usually assigned a score which reflects the associated level of risk. Each risk area may then be assigned a weight which reflects the level of importance in the overall risk calculation relative to other risk areas. Similarly, each control may be assigned a weight which reflects the relative strength of that control. An example of how a FI may approach weighting is shown in **Appendix I.**

For example, if the focus of a business division within a FI is correspondent banking and a proportion of its client base is in different international jurisdictions, geography, therefore, may be considered of higher relevance (and therefore receive higher weight) than client type for that business division. Similarly, certain controls have a more direct impact on the mitigation of ML risk, such as front line controls where client due diligence is weighted more heavily than controls around independent testing.

6.3.2 Reporting & Communication of Results

The results of the ML risk Assessment should be communicated by the AML Unit to relevant stakeholders and business divisions, including but not limited to the Group's senior management and Group Internal Audit. Regulatory and supervisory authorities should be advised as appropriate. Across the industry, there has also been an increased focus on the levels of Operational Risk Capital held by FIs and the results of the Risk Assessment may provide a useful input into the calculation of each FI's Operational Risk Capital.

As a result of the volume of data that will underpin any ML risk Assessment, the methodology should be designed so that the results can be presented in a number of different ways, highlighting risks by any factor recorded, for example by business division, product type, geography or client types, amongst others. This is more than just an averaging of results, but should be able to highlight inherent and residual risk, as well as control effectiveness, for any part of a FI's business.

6.3.4 Note on Links to Client Risk Rating Approaches

As FIs develop their Risk Assessment approaches, measuring risk more consistently in relation to established risk categories (for example, countries, geographies, products and services, channels, transactions and clients) these risk categories may also be taken into account when establishing an approach for risk rating individual client relationships. For example, if each of these risk categories are used to rate a client relationship, they can derive an overall ML risk score for the client. This score will allow that client to be ranked from a risk perspective relative to the entire client book. A FI should ensure that its internal controls are proportionately aligned to the risks posed by the range of its clients, where the highest risk clients will be the object of the most rigorous AML controls, whether through on-

boarding standards, enhanced due diligence, enhanced monitoring and/or more frequent periodic reviews.

6.3.5 Note on Links to Other Risk Rating/Assessment Models

As risk assessments at a FI can also be undertaken by control functions outside of Compliance, FIs should consider the other risk assessments undertaken and seek to ensure there is a common principles-based approach to execution and reporting of the results of different risk assessments. For example, Operational Risk Frameworks will usually contain scoring and rating methodologies to assist in the assessment of risk on a quantitative and qualitative basis. The assessment of the likelihood and impact of scenarios to measure inherent risk can also be used as a way to identify top inherent risks and rank risks by business line or region. If the Operational Risk Framework at a FI is well established and uses a five-tiered rating methodology for residual risks, as opposed to a three-tiered rating methodology, a FI may choose to follow that approach when conducting its ML risk assessment.

Similarly, Internal Audit functions may also have a particular approach for categorising their findings when conducting audits. The results or actions from a ML risk Assessment may be more meaningful to senior management and easier to understand if the way they are categorised is common across the FI, for example a significant audit finding leads to a 'high' risk rating which would then be consistent with a 'high' risk rated action resulting from the ML risk Assessment.

However, if a FI uses a ML risk Assessment approach which differs to others in use across the FI, the rationale for this must be discussed between the different control functions, the impacts assessed and acknowledged, all of which must be fully documented and supported by senior management.

7. What should a FI do with the issues highlighted during a risk assessment?

Following the completion of a risk assessment exercise, gaps or deficiencies in the control environment may be identified. These should give rise to actions which are prioritised appropriately and tracked centrally. Ownership of these items may stem from all parts of the business but Compliance will have oversight of the completion of these actions.

Actions raised may have a significant impact on the residual risk rating once they are completed and therefore, must receive utmost attention and support from senior management and other relevant stakeholders. It is recommended that, wherever possible, the actions raised are remediated before the next risk assessment is carried out in order to assess whether or not the residual risk position has improved.

Strategic actions are likely to be owned by group or a global business line, compared to tactical actions which are likely to be owned by local business line. Business line acceptance of the money laundering/sanctions/bribery and corruption risks faced is imperative, as they are best placed to effect change to the inherent risk profile and effectiveness of the internal control environment.

The issues highlighted during a risk assessment may inform annual planning, monitoring and testing and management information data across a FI. As such, there should be a sufficiently robust quality assurance process to check whether proposed actions appropriately address the issues raised.

8. What impact should a FI's Risk Assessment have on its Risk Appetite?

A FI's ML risk Assessment should be designed by subject matter experts within the specialist unit responsible, for example, Compliance or AML Unit and endorsed by the FI's senior management. The same applies to other Risk Assessments, including Sanctions and Bribery and Corruption.

The result of the ML risk Assessment will explain the current residual ML risk being assumed by the FI. Trending analysis might be performed in order to assess the stability of the portfolio over time and to detect trends.

It is necessary to determine whether the residual risk is equal to the FI's risk appetite for ML risk or whether the residual risk exceeds the FI's risk appetite. In the latter case, measures will need to be agreed in order either to reduce the inherent risk or strengthen the control environment to ensure the residual risk comes back into line with the FI's risk appetite. Alternatively, it may lead to discussion as to whether the FI's risk appetite is correctly positioned. The importance of senior management's involvement is especially critical here, as a FI's risk appetite is a key influence upon its strategic goals and drivers.

A FI's risk appetite may be calibrated against other factors outside of the ML risk Assessment Programme. For example, a set of scenarios and/or examples of risks/unwanted events which are relevant for the FI can be described and articulated to include a threshold impact amount, for example, an acceptable level of loss per annum as a result of civil litigation.

Nevertheless, an example set of scenarios that could form part of a risk appetite evaluation and discussion with senior management could include defining expectations (risk appetite) and reporting on success and/or shortcomings (residual risk) with respect to the following risks: reputation, regulatory, civil liability and criminal liability:

1) Reputation Risk Damage: reputational damage can arise in numerous ways which affects the good reputation of a FI. A FI's reputation in this area is usually negatively affected by the announcement of a serious investigation into money laundering, usually in connection with client accounts and/or transactions, which has, or is likely to have, a significant financial impact through regulatory, civil or criminal monetary fines and penalties. Reputation can also be negatively affected by existing and prospective clients, where negative allegations, including criminal allegations, are made, for example, banking corrupt Politically Exposed Persons, facilitating terrorist finance transactions or dealing with questionable regimes.

2) Regulatory Risk Damage: regulatory rules are constantly evolving and expectations increasing as to what a reasonable risk based AML programme looks like. Examination and testing experiences are also increasing in number, frequency, depth and intensity. The standard expected by regulators has largely shifted from accepting good or common practice to expecting the highest implemented standards as the norm. As these expectations have increased, it has become more difficult to implement a truly risk-based approach if judgements are made on a rules-based foundation. Costs for remediation and look-backs before regulatory censure can be substantial. Regulatory fines and penalties are being much more frequently levied for violations, often involving a number of regulatory agencies who take action for the same or similar issues. Part of this action is also likely to involve a commitment to undertake ongoing actions, including having a team appointed by regulators to be focused on ongoing monitoring of remediation of actions in situ at the FI.

3) Civil Liability Risk Damage: the possibility of legal damages being incurred is increasing with more frequent civil class action lawsuits notably with respect to Sanctions matters, or terrorism finance cases, as well as financial fraud liability for constructive trust, or civil action for failing to comply with a bank mandate.

4) Criminal Liability Risk Damage: while once very exceptional, the prospect of criminal liability risks for ML weaknesses at a FI can no longer be discounted. The phrase "too big to jail" is one that grates amongst many who advocate criminal prosecutions and individual criminal liability as the only way to ensure satisfactory focus and full compliance by FIs with laws, regulations and expectations.

No matter how the results of a ML risk Assessment are compared against a FI's risk appetite, resulting actions should be made clear. It is, therefore, a critical part of the process that roles and responsibilities are clearly defined to ensure that if risks taken are beyond both the appetite and the remit of the control framework, then a consequence management/procedure is in place.

9. What software/systems can be used to conduct a risk assessment?

Some FIs may find it useful to utilise systems or software when conducting a risk assessment. Determining the best system or software to use can be one of the more challenging aspects of conducting a risk assessment. The software employed by FIs varies widely, from customized templates built in standard spreadsheet software to sophisticated database systems built in-house or purchased from vendors. Each approach has relative strengths and weaknesses, and selecting the right tool will depend on various factors, including the size and complexity of the FI (and the corresponding complexity of the assessment itself), the number and geographic distribution of participants in the assessment process, the extent of quantitative metrics/key risk indicators underlying the assessment, the required management information regarding the results of the assessment and the level of dynamic, ongoing changes to the assessment that are anticipated.

The most common challenges in using standard spreadsheet software are the lack of an underlying database, the extensive manual calculations and formulas that must be built and the general single-user nature of spreadsheets. Vendor or in-house built systems, alternatively, typically provide considerably more robust reporting and update features, but can often be difficult to customise. Whichever approach is chosen, and whether a system or piece of software is used at all, FIs should undertake adequate testing ahead of a risk assessment to ensure that it is operating effectively.

Notes

When conducting a risk assessment, other factors may have an impact on the final results which are independent from the qualitative and quantitative factors used by the FI. For example, regulatory impact in relation to one aspect of AML may cause a FI to upgrade the inherent risk rating or downgrade the residual risk rating. Any override mechanism should be clearly documented within a FI's risk assessment methodology to allow for this to occur and it should only be used in exceptional circumstances. Other external drivers may include regulatory speeches or papers, outcomes from the industry or investigative journalism articles. Risk assessments are a subjective assessment and so are open to interpretation. This interpretation can differ between a FI and a regulator, for example.

Such an approach will continue to underpin the value of undertaking risk assessments as a means of maintaining well established standards, identifying potential areas for deficiency, the remediation of those deficiencies and embracing a culture of compliance.

Wolfsberg FAQs on Risk Assessments for ML, Sanctions and Bribery & Corruption Appendices

All of the Appendices below include examples of risk rating approaches for the different categories mentioned throughout this document. The examples serve to illustrate parts of a risk assessment methodology that could be applied by a FI, however, the FI should fully document their approach for arriving at risk ratings within their risk assessment methodology. **The examples provided are neither exhaustive nor binding.**

Appendix A: Glossary

AML Unit	Usually has primary responsibility for the initiation and delivery aspects of the AML programme within a FI. In the context of Risk Assessment, this would include tasks such as methodology development, maintenance, periodic process/activity initiation and record keeping of completed assessments.
Calendar Year	Calendar year refers to January through December of a given year; if the term "calendar year" is not applicable in your country, please use the equivalent 12 month period from January through December of the previous year.
Counter Terrorist Financing (CTF)	The measures put in place to prevent those involved in the financing and perpetration of terror and terror-related activity from accessing financial services.
Client	Individuals: Individuals with an account, product or service. Entities: Natural persons, company, trust, charity, partnership, or sole trader with a FI account, product or service.
Client Due Diligence (CDD)	The process of implementing policies and procedures that are designed to help monitor and evaluate the illicit finance risk posed by a client. Client due diligence can include, but is not limited to: establishing the identity of clients, determining expected client behaviour, and/or monitoring account activity to identify those transactions that do not conform with the normal or expected transactions for that client or type of account.
Client Risk Rating	Assessment of the money laundering/terrorist financing risk posed by each client in order to understand the risks faced by the firm. The client risk rating may also be used to determine the different treatments of identification, verification, additional client information, monitoring and periodic review required.
Enhanced Due Diligence (EDD)	Additional information collected as part of the client due diligence process or increased cautionary measures, such as ongoing monitoring of activity, applied on a risk-sensitive basis in any situation which, by its nature, can present a higher risk of money laundering or terrorist financing. The extent of additional information sought, and of any monitoring carried out, in respect of any particular business relationship, or class/category of business relationship, will depend on the money laundering or terrorist financing risk that the client, or class/category of business relationship, is assessed to present to the firm.
Inherent Risk	Represents the exposure to money laundering, sanctions or bribery and corruption risk in the absence of any control environment being applied.

Internal Controls	Policies, procedures, systems and personnel in place within a FI, designed to protect against the materialisation of a ML risk, or to ensure that risk factors are promptly identified.
Know Your Client (KYC)	Policies and procedures used to determine the true identity of a client and the type of activity that is "normal" for that client.
Monitoring	An element of a FI's anti-money laundering program in which client activity is reviewed for unusual or suspicious patterns, trends or outlying transactions that do not fit a normal pattern. Transactions are often monitored using software that weighs the activity against a threshold of what is deemed "normal and expected" for any given client.
Residual Risk	The risk that remains after controls are applied to the inherent risk. It is determined by balancing the level of inherent risk with the overall strength of the risk management activities/controls. The residual risk rating is used to assess whether the ML risks within the FI are being adequately managed.
Risk Assessment	A risk assessment is an exercise used to identify key risks faced by the firm and to test the controls that a firm has in place to mitigate these risks. Risks can be both external and internal to the firm. The risk assessment aims to measure the total exposure a firm has to the risks it faces and to plan actions to reduce these risks.

Appendix B: Example Process for a Risk Assessment

The examples serve to illustrate parts of a risk assessment methodology that could be applied by a FI, however, the FI should fully document their approach for arriving at risk ratings within their risk assessment methodology. **The examples provided are neither exhaustive nor binding.**

1. Define the inherent risk factors
2. Weight the inherent risk factors as per methodology
3. Collect the data and subject it to appropriate review
4. Score the inherent risk factors to arrive at both
    a. an individual risk category rating, e.g. High, Moderate, Low (HML); and
    b. an overall HML score
5. Define the control effectiveness categories
6. Identify all the controls and map either to:
    a. the Controls categories:
        i. Weight the Categories based on importance, number of controls, number of key controls; and
        ii. Score the control effectiveness by aggregating the results to get an overall HML score; OR
    b. the Inherent risk categories:
        i. Weight the controls based on importance, key Controls.
        ii. Map the Controls to each of the Inherent risk categories and score those controls in aggregate against each risk category; and
        iii. Aggregate the control effectiveness categories to get an overall HML score;
7. Note and record the shortcomings or weaknesses in each of the identified controls for future remediation work (see 10 below)
8. Take the overall inherent risk score and apply the controls effectiveness score by applying the residual risk matrix
9. Arrive at the residual risk and determine at the appropriate governance body whether the residual risk is within FI tolerance or risk appetite; and
10. Determine the remediation action plan covering those items in 8 above that are determined as being in need of further action, by whom and by when.

Appendix C: Example Client Inherent Risk Ratings

The examples serve to illustrate parts of a risk assessment methodology that could be applied by a FI, however, the FI should fully document their approach for arriving at risk ratings within their risk assessment methodology. **The examples provided are neither exhaustive nor binding.**

Clients 1 – Persons	Rating
Individuals	
- HNW	High
- Retail	Low
- Other	Moderate
Entities	
Publicly Held Companies	
- Recognised Stock Exchange	Low
- Not Recognised Stock Exchange	Moderate
Privately Held Companies	
- Operating Company	Low
- Non-Operating Company	Moderate
- Bearer Share Company	High
Government Entities	
- Domestic	Low
- Medium Risk Country	Moderate
- High Risk Country	High
- Higher Risk Country	Higher
Financial Institutions/Banks and Regulated Brokers	
- Recognised Stock Exchange plus Compliant Country	Low – Moderate
- Partially Compliant and not Compliant Country	Moderate
- Not-Recognised Stock Exchange and not Compliant Country	High/Higher

* Note, a four point rating scale is used within the above example and can differ depending on the rating scale chosen.

Clients 2 – Special Categories with Increased Risk Attributes	Rating
Politically Exposed Person[7]	
- Domestic	Moderate
- International	High
Industry	
- Money Services Businesses	Moderate/High
- Charities and Non-Profit Organisations	Moderate/High
- Intermediaries/Commission agents	Moderate/High
- Real Estate Agents	Moderate/High
- High Value Goods Dealers	Moderate/High
- Precious Metals & Stones Dealers	Moderate/High
- Gatekeepers	Moderate/High
- Casino's, including Internet Gambling	Moderate/High
- Arms Dealers	Moderate/High
- Private Military Firms	Moderate/High
- Digital Currency Providers or similar	Moderate/High

[7] Also as per minimum regulatory requirements

Appendix D: Example Products, Services and Transactions Inherent Risk Ratings

The examples serve to illustrate parts of a risk assessment methodology that could be applied by a FI, however, the FI should fully document their approach for arriving at risk ratings within their risk assessment methodology. **The examples provided are neither exhaustive nor binding.**

Examples of Increased Risk Products & Services	Rating
Alternative Investment/Structured Products	Moderate/High
Trade/Export Finance	Moderate/High
International Private Banking/WM	High
International Correspondent Banking	High
- International Wires	High
- Pouch Services	High
- Precious Metals (Physical Delivery)	High
- Banknotes	High
- Payable-through Accounts	High
- Downstream Clearing	High
Special Use Accounts	High
International Brokered Deposits	High
Safe Deposit Services	High
Precious Metals (Delivery) Services	High
Unlimited Cards	High
Benchmark and Other Setting of Indices	High

Examples of Increased Risk Transactions	Rating
Significant/Unusual Cash/Cash Like	High
Pass-through Transactions	High
Nested accounts	High
International Wires to High Risk Countries	High
Suspected Shell Company Transactions	High
Rapid In/Out (High Velocity Turnover)	High
Unusual Wire Transfers	High
Smurfing	High
Suddenly Active	High
Other Unusual/Suspicious	High

Appendix E: Example Inherent Risks for Channels risks

The examples serve to illustrate parts of a risk assessment methodology that could be applied by a FI, however, the FI should fully document their approach for arriving at risk ratings within their risk assessment methodology. **The examples provided are neither exhaustive nor binding.**

Channels Risk	Rating
Account Origination	
- Solicited	Low
- Unsolicited (including walk-ins)	High
Account Servicing	
- Face-to-face	Low
- Only non-face-to-face* (including mail, phone, text, video, internet)	Moderate*/High
- Only non-face-to-face via Intermediary, including Gatekeepers	Moderate

* If a client is known to the FI but conducts their business activity non-face-to-face.

Appendix F: Example Inherent risks for Geography/Country Risks

The examples serve to illustrate parts of a risk assessment methodology that could be applied by a FI, however, the FI should fully document their approach for arriving at risk ratings within their risk assessment methodology. **The examples provided are neither exhaustive nor binding.**

Geography/Country Risk	Rating
Own Bank/FI Locations	
- Higher Risk Countries	Higher
- High Risk Countries	High
- Moderate Risk Countries	Moderate
- Low Risk Countries	Low
Client Locations	
- Higher Risk Countries	Higher
- High Risk Countries	High
- Moderate Risk Countries	Moderate
- Low Risk Countries	Low

* Note, a four point rating scale is used within the above example and can differ depending on the rating scale chosen.

Appendix G: Example Inherent Risks for other Qualitative Risks

The examples serve to illustrate parts of a risk assessment methodology that could be applied by a FI, however, the FI should fully document their approach for arriving at risk ratings within their risk assessment methodology. **The examples provided are neither exhaustive nor binding.**

Other Qualitative Risk Factors	Rating
Client Base Stability	Low/Moderate/High
Integration of IT Systems	Low/Moderate/High
Expected Account/Client Growth	Low/Moderate/High
Expected Revenue Growth	Low/Moderate/High
Recent AML Compliance Employee Turnover	Low/Moderate/High
Reliance on Third Party Providers	Low/Moderate/High
Recent/Planned Introduction of New Products and/or Services	Low/Moderate/High
Recent/Planned Acquisitions	Low/Moderate/High
Recent Social Projects and Initiatives Related to AML Compliance Matters (e.g. Remediations, Eliminations of Back-logs, Offshoring)	Low/Moderate/High
Recent Internal Audit or Other Material Findings	Low/Moderate/High

Appendix H: Example Standard Inherent Risk Ratings (Major Bank/FI Businesses)

The examples serve to illustrate parts of a risk assessment methodology that could be applied by a FI, however, the FI should fully document their approach for arriving at risk ratings within their risk assessment methodology. **The examples provided are neither exhaustive nor binding.**

Standard Inherent Risk Ratings	
FI Type / Business Unit / Business Line	**Inherent ML risk Rating (3 tier)**
Asset Management	Low to Moderate
Brokerage	Moderate to High
Commercial Banking	Moderate to High
International Correspondent Banking	High
Credit & Other Card Banking	Low to Moderate
Investment Banking	Low to Moderate
Retail Banking	Moderate to High
Wealth Management / Private Banking	Moderate to High

Appendix I: Example Factor Weightings

The examples serve to illustrate parts of a risk assessment methodology that could be applied by a FI, however, the FI should fully document their approach for arriving at risk ratings within their risk assessment methodology. **The examples provided are neither exhaustive nor binding.**

Inherent Factor Weighting Examples

Inherent Factor Weighting Examples	
Inherent Factor	**Inherent Weighting**
Channels	5-10%
Clients	25-35%
Country / Geography	20-30%
Products & Services	20-30%
Other Qualitative Risk Factors	10-15%

Control Factor Weighting Examples

Control Factor Weighting Examples	
Control Factor	**Control Weighting**
KYC (incl. All requirements)	20-30%
Monitoring & Controls	20-30%
Policies & Procedures	10-15%
Other Risk Assessments	10-15%
AML Corporate Governance; Management Oversight & Accountability	5-10%
Management Information / Reporting	5-10%
Record Keeping & Retention	5-10%
Designated AML Compliance Officer / Unit	5-10%
Detection and SAR Filing	5-10%
Training	5-10%
Independent Testing & Oversight	5-10%
Other Controls / Others	5-10%

Appendix J: Example Calculation of Residual Risk

The examples serve to illustrate parts of a risk assessment methodology that could be applied by a FI, however, the FI should fully document their approach for arriving at risk ratings within their risk assessment methodology. **The examples provided are neither exhaustive nor binding.**

3-tier Residual / Risk Rating Approach

Example Calculation of Residual Risk		
Inherent Risks	**Controls Strength**	**Residual Risks**
Low	90-100%	**Low**
	89-80%	**Moderate**
	<80%	**High**
Moderate	90-100%	**Low**
	89-80%	**Moderate**
	<80%	**High**
High	90-100%	**Low**
	89-80%	**Moderate**
	<80%	**High**

5-tier Residual Risk Rating Approach

Example Calculation of Residual Risk		
Inherent Risks	**Controls Strength**	**Residual Risks**
Low	95-100%	**Low**
	90-94%	**Low to Moderate**
	85-89%	**Moderate**
	80-84%	**Moderate to High**
	<80%	**High**
Moderate	95-100%	**Low**
	90-94%	**Low to Moderate**
	85-89%	**Moderate**
	80-84%	**Moderate to High**
	<80%	**High**
High	95-100%	**Low**
	90-94%	**Low to Moderate**
	85-89%	**Moderate**
	80-84%	**Moderate to High**
	<80%	**High**