For internal use only

Schedule 11

DR NAGY CONSULTING QFC BRANCH

Manual for Internal Risk Assessment

September 2020

Adopted with Founder's Resolution nr. 2/2020
Approved by Dr. Nagy E. Peter, P.h.D. managing director on 1 September 2020

Effective from 1 September 2020

TABLE OF CONTENT

I. INTRODUCTION

I.1. Purpose

This manual for business risk assessment ("**Manual**") has been designed to determine the risk assessment of Dr Nagy Business Consulting QFC Branch (hereinafter referred to as the **"Company"**) as part of its risk management procedure, in accordance with applicable law and ensure good industry practice through a proportionate, "risk-based" approach. The overall aim of this assessment is to identify any area of vulnerability with regard to money laundering and to create a complete profile of any risks posed to the Branch.

The purpose of this Manual is to implement adequate internal procedures and controls that ensure the identification, analyses, management and mitigation of inherent risks associated with illicit activities (such as money laundering and terrorist financing) the Branch may face during its activities. The Manual helps the Branch to identify where the Branch is vulnerable to risks of money laundering and terrorist financing and ensures that corresponding resources are deployed and adequate systems are in place to support the controls needed to identify, assess and manage risks and therefore lower the Branch's risk exposure.

The results of the risk assessment process set out by this Manual will also be used to:

1. identify vulnerabilities of the Branch and any gaps in the AML/CFT Policy;
2. improve the AML/CFT Policy and related procedures and mechanisms;
3. assist senior management with: (a) strategic decisions; (b) making reasonable, informed decisions about determining risk appetite;
4. implementation of control mechanisms, allocation of resources and technology;
5. develop risk mitigation strategies, internal controls;
6. ensure that regulators are made aware of the key risks, control gaps and remediation efforts of the Branch.

This Manual is to be used in conjunction with the *"Policy on the prevention and countering of money laundering and terrorist financing and on the implementation of financial and proprietary restrictive measures ordered by the UN Security Council"* (hereinafter referred to as the "**AML/CFT Policy**") of the Branch as a supplement of Schedule V.9. (*Internal risk assessment*) of the AML/CFT Policy, intended for internal use only. Terms not otherwise defined in this Manual shall have the meaning attributed to them in the AML/CFT Policy.

I.2. Scope of risk assessment

The Branch, its senior management and the MLRO shall ensure that adequate resources, funds and systems are in place to support the controls needed to identify, assess and manage risks with respect to each of its licensed business activities of the Branch, namely:

1. provision of company headquarters services;
2. provision, formation and administration of trusts and similar arrangements of all kinds;
3. provision, formation, operation and administration of companies; and
4. provision of the following professional services:
   - advisory/consulting in relation to strategic consulting; and
   - third party administration.

The Branch implemented an integrated risk assessment procedure that considers the complexity and nature of its business lines and relies on the three fundamental principles of subsidiarity, transparency and consistency, as set out in this Manual.

The Branch carries out risk assessment in respect of each of its business activities separately.

I.3. Place of risk assessment within the risk management framework

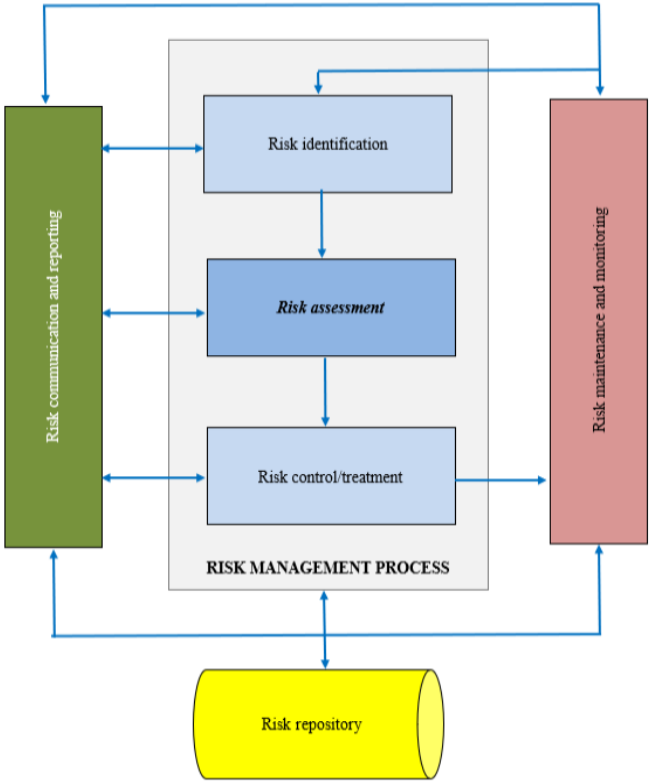
The Branch's risk management framework is comprised of:

1. The **risk management process** in which risk identification, assessment and treatment (mitigation/acceptance) are the first line of defense for the Branch. The MLRO is responsible for the implementation and the compliance of the process. The cooperation of other employees and engagement with other Company relevant functions (e.g. IT) are essential for an accurate quantification of the risk. The senior management must be made aware of the risks that the Branch is facing and must validate the risks and agree on mitigation plans where risks are assessed as out of tolerance.

2. The **risk repository is** a repository of all identified risks in the Branch recorded and stored for at least ten years separately for each business activity. The MLRO is the owner of this repository and must ensure that its content is updated with appropriate details to facilitate the risk maintenance, monitoring and reporting activities.

3. The **risk monitoring and periodical reassessment**. The MLRO is also accountable for this periodical activity. A key activity is the update of the information on existing risk acceptance forms and on mitigation plans documented in the risk repository. During this phase, further actions could be identified and documented to reduce the risk. Periodical reassessments of risks are needed to ensure that information is complete and consistent.

4. The **risk communication and reporting.** It is composed by all activities performed to report and to communicate about risks to ensure transparency of risks.



II. RISK ASSESSMENT

II.1. Roles

The MLRO is responsible for the assessment of risks. All stages of the risk assessment must be recorded, and approval/authorization must be obtained from the managing director, where applicable.

The finalised risk assessment is reviewed and approved by the managing director, in each case.

II.2. Frequency of risk assessment

The MLRO shall perform, review and document a risk assessment:

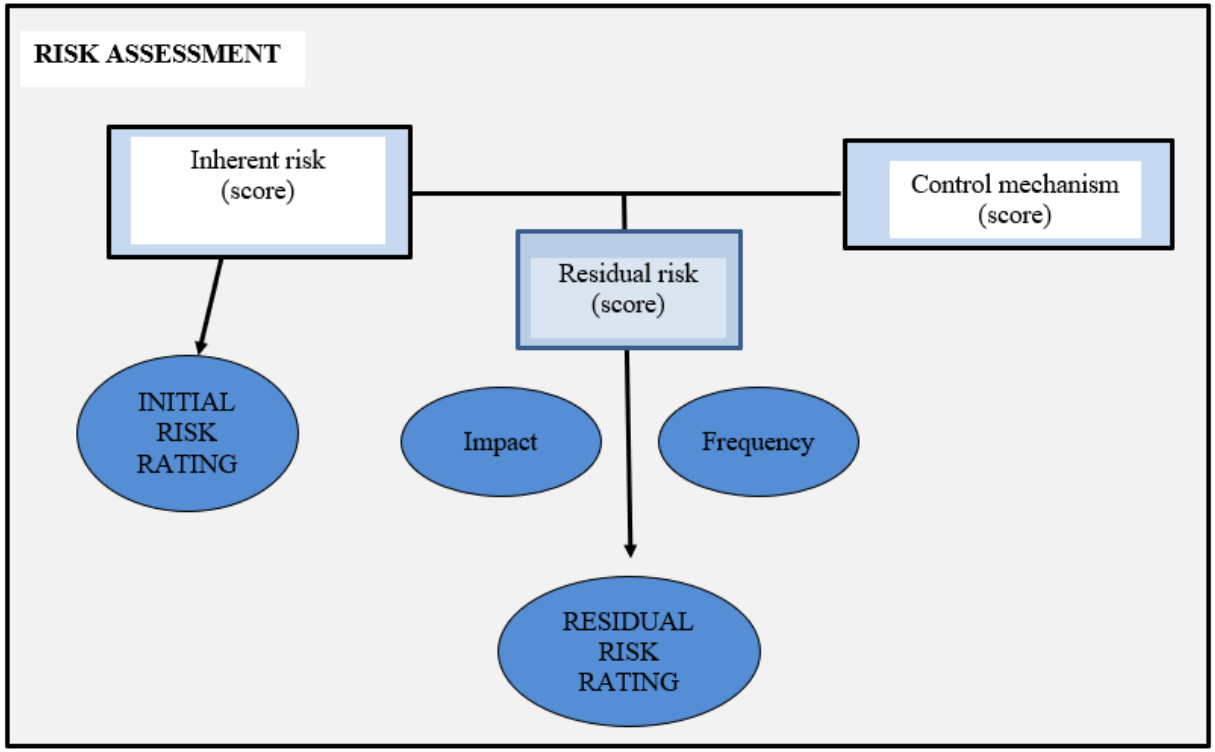
a) at least annually;
b) as required/if triggered (e.g. a new Client's risk profile shall be evaluated when first becoming a Client);
c) on an ad hoc basis;

and shall report to senior management on the results annually (unless otherwise required in this Manual) in the Annual MLRO Report.

II.3. Risk assessment method and stages

The goal of the business risk assessment is the quantification of the level of risk the Branch is exposed to. The Branch follows recognized standards and risk management frameworks pursuant to which a risk rating is expressed as a combination of the impact of the risk event and its likelihood to happen.

As a first step of the assessment process the Branch determines the inherent risks within the different categories that may arise in respect of a Client/transaction and evaluates them pursuant to score tables and determines an initial risk rating by applying the below RAG matrix. The initial risk score serves as a basis for the determination of the **initial risk rating** (inherent risk rating) for that risk pursuant to a RAG matrix which considers the impact (inherent risk score) and the possible frequency of that given risk. Following this, the Branch identifies the adequate control mechanisms for each risk, assigns a score to them based on their effectiveness (and as per the score table) and balances their respective accumulated scores with the inherent risk score in order to arrive at a residual risk score for the given risk. The residual risk score serves as a basis for the determination of the **residual risk rating** which is calculated by applying the RAG matrix once again.



The Branch uses the following multi-stage approach to perform a risk assessment:

- **Stage 1**. *Identification of inherent risk factors and vulnerabilities (collection of data to subject it to appropriate review)*
- **Stage 2**. *Determining inherent risk scores and initial risk rating*
- **Stage 3.** *Assessing the control environment and relevant scores (and recording weaknesses for future remediation)*
- **Stage 4.** *Determining residual risk score*
- **Stage 5.** *Determining residual risk rating and next steps in light of the Branch's risk appetite*
- **Stage 6.** *Development & implementation*
- **Stage 7.** *Monitoring & review*

Stages of risk assessment:

Stage 1. Identification of risk factors and vulnerabilities

The Branch categorizes risks as follows and considers the following aspects in relation to each risk during their evaluation:

RISK AREA	POINTS OF CONSIDERATION
Services	• Types of assets handled potentially handled by the Branch • Services offered by the Branch that enable money to be placed in the business, or moved from/through it • Services offered by the Branch that may enable ownership of assets to be disguised • The service involves company/trust management • The service involves or may involve the provision of nominee directors, nominee shareholders or shadow directors, or the formation of companies in a third country • The service or transaction is one which might favour anonymity • Nature of services offered • Activities undertaken

	• Types of business relationship • Adequate systems (e.g. IT) and backup plans
Interface risk	• The transaction/service may involve non-face-to-face business relationships or transactions, without certain safeguards, such as an electronic identification process which meets the conditions set out in applicable law • Delivery/communication/direction channels (especially where remote or new) • New business practices • New services or delivery mechanisms
Country risk ***(Branch)***	• Possible risks arising from the fact that the services are provided and the activities are carried out in Qatar • Reasons why Qatar may be attractive for investments • Quality of neighbouring countries (e.g. providing funding or support for terrorism)
Geographical risks ***(Client)***	• Geographical location of Client and Client business • High risk countries (*consider and review: UN sanctions, Basel AML Index, FATF's high-risk and un co-operative jurisdictions ,OECD's list of un co-operative tax havens, the Financial Secrecy Index, Transparency International's Corruption Perception Index, EU, UK and USA sanctions, World Bank World Governance Indicators, Fragile States Index, Global Terrorism Database) other relevant assessments of the applicable financial markets authorities)* • Countries with no/little AML regulations *(FATF)* • Countries subject to sanctions, embargos, or similar measures • Countries providing funding or support for terrorism

Client risk	• Types of Client • The ownership structure of the Client • The corporate structure of the Client is unusual or excessively complex given the nature of the Branch's business • The industry the Client runs its business(es) in (*e.g. cash sensitive businesses*) • Location of Client • The business relationship is conducted in unusual circumstances • How Client is introduced • Where Clients' funds come from • Where Clients' funds go to • Clients' background & due diligence checks • Verification of Clients' identity (or company validation) • Client referral • Client investment behaviour *(i.e. large cash transactions; one-off transactions; regular transactions with the same individual(s), small amount transactions frequently)* • Clients from high-risk sectors or businesses • Politically exposed persons (PEP's) • Clients seeking anonymity • Remote Clients • The Client is a legal person or legal arrangement that is a vehicle for holding personal assets • The Client is a company that has nominee shareholders or shares in bearer form
Other qualitative risk factors	• Client base stability of the Branch • Integration of IT systems • Expected account/Client growth of the Branch (within specific time range) • Expected revenue growth of the Branch • Recent (AML compliance) employee turnover (if any) • Employee risks • 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

Stage 2. Determining inherent risk scores

Once we identify each risk, we then assess the risk by determining its potential impact and attribute a score to it (as well as record the reasoning, origin, nature, particularity and severity of that risk).

The risk impact estimation identifies the potential consequence of the risk. In general, the Branch uses the following score table:

Result of Impact Estimation	Impact score
Very highly serious harm	**5**
Very serious harm	**4**
Serious harm	**3**
Minor harm	**2**
No significant harm	**1**

The Branch considers and evaluates the impact of the risks from the perspective of each of its business activities separately. The following score tables aim to determine the inherent risks the Branch may face during its operations carried out in each of its business activities exhaustively and were arrived to after careful consideration of the complexity and size of its activities. Nevertheless, it might be the case that a Branch employee encounters unprecedented events and risk factors, in which case such employee shall consult the Branch's MLRO for further guidance on a case-by-case basis. The present manual shall be updated with the results of such unprecedented procedure and experience.

A. Risk area: Services

RISK SCENARIO	IMPACT SCORE (IN RESPECT OF EACH BUSINESS ACTIVITY)				
	Headquarter services	*Provision, formation and administration of trusts*	*Provision, formation, operation and administration of companies*	*Strategic consulting and advisory*	*Third party administration*
An undue level of secrecy is requested during the provision of the service	5	5	5	5	5
There is no clear commercial rationale of the Client requesting the service	5	5	5	5	5
Client is hesitant to provide all requested KYC, AML/CTF information	5	5	5	5	5
Legal source of handled assets during the service is unclear	n/a	5	5	n/a	n/a
Service provided to the Client is primarily related to wealth management	n/a	4	4	3	3
Intermediaries are used from the Client's side when using the Branch's services	4	4	4	4	4
The service enables money to be placed in the business	n/a	3	3	2	n/a
Electronic money, decentralized electronic currency is involved with the transaction	2	4	4	3	3

Ability to disguise ownership of assets / favours anonymity	n/a	5	4	n/a	n/a
The service involves the provision of nominee directors, nominee shareholders or shadow directors, or the formation of companies in a third country	5	5	5	n/a	n/a
The transaction has a high value transaction (volume or value)	n/a	2	2	2	2
The transaction is a one-off transaction (or does not fit with the Client's overall commercial behaviour)	3	4	4	4	3
The Client is accepting of high charges and/or penalties during operations	2	2	2	2	2
Enters into transactions that do not make commercial sense	4	4	4	4	4
The transaction is unusual or complex	4	4	4	4	3
The transactional patterns of the Client are otherwise odd	2	2	2	2	2
Source of fund cannot be easily verified	3	4	4	3	3
Aggregated frequent and small transactions	2	2	2	2	2
Remote control of transactions by Client	2	4	4	3	2

B. Risk area: Interface

RISK SCENARIO	IMPACT SCORE (IN RESPECT OF EACH BUSINESS ACTIVITY)				
	Headquarter services	*Provision, formation and administration of trusts*	*Provision, formation, operation and administration of companies*	*Strategic consulting and advisory*	*Third party administration*
The situation involves non-face-to-face business relationships or transactions (without certain safeguards, such as an electronic identification process)	5	5	5	5	5
Client due diligence is carried out by third parties/intermediaries	4	4	4	4	4
Relationship with the Client is otherwise indirect/through an intermediary	4	4	4	4	4
Client gives investment and other orders/directions by phone, fax, e-mail or via electronic means by logging in to his personal online profile	1	4	4	3	2
New marketing/ sales channels of services	1	1	1	1	1

C. Risk area: Country of Branch's registered seat

RISK SCENARIO	IMPACT SCORE (IN RESPECT OF EACH BUSINESS ACTIVITY)				
	Headquarter services	*Provision, formation and administration of trusts*	*Provision, formation, operation and administration of companies*	*Strategic consulting and advisory*	*Third party administration*
Corruption in Qatar is relatively low and is among the lowest in the Middle East and North African region. Transparency International Corruption Index 62/100 World Governance Indicator – Control of Corruption 77	1	1	1	1	1
Qatar is not on the FATF List of Countries that have been identified as having strategic AML deficiencies	0	0	0	0	0
Qatar was deemed a Jurisdiction of Concern by the US Department of State 2016 International Narcotics Control Strategy Report (INCSR). Findings: - Qatar still has a largely cash economy. - The expansion of the financial and trade sectors, the large number of expatriate laborers who send remittances to their home countries, the liberalization and growth in the real estate sector, uneven corporate oversight, and Iran's efforts to bypass sanctions through Gulf	4	4	4	4	4

increasingly vulnerable to the threat of money laundering. - The exploitation of charities and private donations to finance terrorism continues to be a concern, as does the ability of individuals to bypass the formal financial sector for illicit financing.					
Saudi Arabia, Bahrain, the United Arab Emirates UAE, Egypt, Yemen, Libya's eastern-based government and the Maldives all cut diplomatic ties with Qatar claiming it supported "terrorism" and was too close to Iran.	4	4	4	4	4
Qatar is not on EU White list equivalent jurisdictions	3	3	3	3	3

D. Risk area: Geography

RISK SCENARIO	IMPACT SCORE (IN RESPECT OF EACH BUSINESS ACTIVITY)				
	Headquarter services	*Provision, formation and administration of trusts*	*Provision, formation, operation and administration of companies*	*Strategic consulting and advisory*	*Third party administration*
Client is based in, or conducting business through or in, a high-risk jurisdiction and/or a jurisdiction known to suffer from corruption	4	4	4	4	4

Beneficial owners of a legal person Client are resident in a high-risk jurisdiction	4	4	4	4	4
Client makes or accepts payments (for example, electronic transfers) to or from offshore accounts	3	3	3	3	3
Client has access to offshore funds (for example, cash withdrawal or electronic funds transfer)	3	3	3	3	3
Client's business is registered in a foreign jurisdiction with no local operations	3	4	4	3	3
Client is represented by another person in another jurisdiction, such as under a power of attorney	2	2	2	2	2
Client is based in, or conducting business through or in countries or geographic areas identified by FATF Statements as having weak AML/CFT regimes, and for which financial institutions should give special attention to	4	4	4	4	4

transactions					
Client is based in, or conducting business through or in countries or geographic areas subject to sanctions, embargoes, or statements of concern issued by international bodies such as the United Nations, FATF, or governments.	5	5	5	5	5
Client is based in, or conducting business through or in countries or geographic areas identified by credible sources as lacking appropriate AML/ CFT laws, regulations and other measures	5	5	5	5	5
Client is based in, or conducting business through or in countries or geographic areas identified by credible sources as providing funding or support for terrorist activities or that have designated terrorist organisation operating within them	5	5	5	5	5
Client is based in, or conducting business through or in countries or geographic areas where protection for Client privacy prevents the effective implementation of AML/CFT requirements and/or facilitates the framework for	5	5	5	5	5

companies or the issuance of bearer shares and/or prevent effective information sharing and international cooperation					
Cross border elements: the Branch, Client and the beneficiary of the contract are in separate jurisdictions	2	2	2	2	2
Countries with effective AML/CTF systems (e.g. EU member states) in line with international standards	1	1	1	1	1
Countries with low levels of corruption (based at least on the World Bank's Governance Indicators index)	1	1	1	1	1

E. Risk area: Client

RISK SCENARIO	IMPACT SCORE (IN RESPECT OF EACH BUSINESS ACTIVITY)				
	Headquarter services	*Provision, formation and administration of trusts*	*Provision, formation, operation and administration of companies*	*Strategic consulting and advisory*	*Third party administration*
Client involved in a complex business ownership structure with no legitimate commercial rationale.	5	5	5	5	5

Client that is a legal person (trust, company or other legal arrangement) has a complex business structure with little commercial justification, which obscures the identity of UBOs of the Client.	5	5	5	5	5
Client is in a position that may expose them to corruption.	4	4	4	4	4
Client is engaged in a cash intensive business.	2	3	3	3	2
Client is a PEP.	4	4	4	4	4
Source of funds and wealth is difficult to verify.	4	4	4	4	4
There is no commercial rationale for a Client buying the products that it seeks, or the Client requests undue levels of secrecy/business relationship is otherwise unusual	5	5	5	5	5
BOs of a legal person are difficult to identify and/or verify.	4	4	4	4	4
There is a one-off transaction in comparison with an ongoing business relationship or series of	3	4	4	3	3

Client is resident in a high-risk country	5	5	5	5	5
Client has a dual nationality, and at least one is from a high risk jurisdiction.	5	5	5	5	5
Client makes or accepts payments (for example electronic transfers) to or from accounts that have not been identified by the Branch.	5	5	5	5	5
Client, when migrating from one product or service to another, carries a different type and level of ML/TF risk.	1	1	1	1	1
Client has income which is not employment-based or from a regular known source.	3	4	4	4	3
Client is new rather than having a long- term and active business relationship with the Firm.	1	1	1	1	1
Client is an unregistered charity, foundation or cultural association.	5	5	5	5	5
Client is a bearer share company	5	5	5	5	5

Client is a government entity from higher risk country	4	4	4	4	4
The business of the company is more likely to be subject to money-laundering (e.g.: precious metal, stone dealers; casinos, internet gambling; arms dealers; digital currency providers; agents/intermediary services)	4	4	4	4	4
The Client is recruited on specific targeted conferences	1	1	1	1	1
The Client is recruited based on the recommendation of already existing Clients	1	1	1	1	1
Hidden relationships between Clients evident through investment goals/direction/funds flows	3	3	3	3	3
Client is a company whose securities are listed in a stock exchange and are subject to disclosure requirements, which ensure the adequate transparency of the BO	1	1	1	1	1
Client is residing in low-risk geographical areas	1	1	1	1	1
Client is a majority-state-owned company from lower risk countries	1	1	1	1	1

F. Risk area: Other qualitative risk factors

RISK SCENARIO	IMPACT SCORE (IN RESPECT OF EACH BUSINESS ACTIVITY)				
	Headquarter services	*Provision, formation and administration of trusts*	*Provision, formation, operation and administration of companies*	*Strategic consulting and advisory*	*Third party administration*
Client is not recommended by already existing clients or recruited for usual channels	1	1	1	1	1
Reliance on third party providers for carrying out CDD	3	3	3	3	3
Unstable/insecure/vulnerable IT system	3	3	3	3	3
Recent employee turnover	2	2	2	2	2

The so determined initial risk scores serve as a basis for the determination of the **initial/inherent risk rating** for the given risk pursuant to a RAG matrix set out below. The RAG matrix considers the impact (inherent risk score) and the possible frequency of that given risk to determine whether the inherent risk is rated as low risk, low medium, medium, medium high or high risk.

Stage 3. Assessing the control environment and relevant scores (and recording weaknesses for future remediation)

Once the AML risks and vulnerabilities have been identified and rated, the Branch then identifies and evaluates the adequate solutions, controls and mitigating actions to eliminate, reduce or manage (handle) the risks. The Branch's assessment enables a pre-emptive approach to risk and allows the Branch to apply corrective actions and mitigating controls to effectively handle risks and vulnerabilities.

The Branch aims to eliminate or reduce risks to an acceptable level through the following risk management controls:

1. Elimination

2. Reduction

3. Management/ risk acceptance

In some cases, an identified risk can be eliminated entirely by putting certain controls or systems into place to ensure that the risks are excluded altogether. However, The Branch recognises that it is not possible to eliminate all risks due to the nature of the services it offers, in which cases the Branch aims to reduce them to an acceptable level and/or to have dedicated and adequate controls in place to manage the risk in compliance with applicable law. Where risks remain, the Branch defines and choses the most adequate controls and solutions on a case-by-case (risk-by-risk) basis to manage the outcomes to reduce the risk of money laundering in the Branch to an absolute minimum. With the acceptance of a risk, the management states its understanding of the exposure to the risk.

The Branch considers the following developing controls or managing tools:

CONTROL MEANS	SCORE
KYC procedure (acquiring quality data)	1-3
Standard due diligence procedure on all Clients and business relationships	1-3

Using an enhanced due diligence process for high-risk Clients or business relationships	3-4
Ex-ante application of the sanction list filtering system to check if the Client is in the database or not	3-4
Continuous monitoring of the Client, risks, contract, transactions & controls	1-2
Acquiring additional documents in connection with higher risk contracts	1-2
Policies & procedures (the Branch has a documented enterprise wide AML/CFT Policy that covers all main AML/CFT compliance areas (such as appointment of an AML/CFT officer, risk assessment, policies and procedures, CDD, transaction monitoring). The policy and the methodologies are revised and approved by senior management of the Branch at least annually.)	1-2
Implementing a Client recruiting system that is based on recommendations from already existing Clients/ addressing a specific group of Clients only	3-4
Inquiring on the background and purpose of transactions that exceed predefined thresholds, to ensure alignment with Client's profiles (pre transaction checks)	1-2
AML Corporate Governance; Increased management oversight & accountability through the Branch's escalation and approval procedure (e.g.: obtaining approvals from line managers and/or compliance personnel before executing higher risk transactions)	2-4
Management information / Reporting both inside and to outside of Branch	1-3
Record keeping & retention / continuous reassessment and revaluation of risks	1-3

Designated AML Compliance Officer (MLRO)	1-2
Detection and filing of reports with authorities	1-2
Implementing an employee training program dedicated to money laundering and the risks posed and identified	2
Independent testing & oversight is ensured from time to time	2-3
Carrying out identity and background checks on all Clients and suppliers	2-3
Completing annual CRB, background and financial checks on all employees	2-3
Implementing systems to identify and monitor transaction patterns *(i.e. high value, complex, unusual etc)*	3-4
Identification and monitoring of Clients who are PEPs, beneficial owners and/or beneficiaries	3-4
Signing up to newsletters and notifications from monitoring groups and bodies specific to money laundering and terrorist financial *(i.e. FATF, OFSI etc)*	1
Advanced information technology of the Branch	1
Specific IT actions (e.g. restricting the use of electronic self-help channels offered by the Branch of customers suspected of internet fraud)	2-4
Review Client business activities and associated relationships	1-2

Stage 4. Determining residual risk score

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.

When applying the solutions or controls, the Branch uses the inherent risk score obtained in the risk identification process to ensure that it is clear what the current risk is and what an acceptable level would be in order to apply adequate (both in respect of effect and in number) control solutions. Once all accumulated control and action scores have been subtracted from the inherent risk score, we arrive at the residual risk score.

Once again, the RAG matrix is applied in accordance with the stages set out below to such residual risk score to reach the inherent risk rating (low, low medium, medium, medium high or high) and to determine what actions shall follow.

Stage 5. Determining residual risk rating and next steps in light of the Branch's risk appetite

Estimation of frequency (Likelihood)

The likelihood describes how likely the relevant risk is to occur. This is the expected frequency of the risk factor to take place. This value can be based on statistical information on the specific topic when available, the Branch's relevant experience or on expert opinion.

The following table provides the range of values to be used for the likelihood estimation.

Event	Frequency	Likelihood score
The risk event occurs regularly/always	**Always**	**5**
The risk event occurs frequently (i.e. multiple times a year)	**Very Likely**	**4**
The risk event is known, can happen and will happen once a year to five years (over multiple years)	**Likely**	**3**
The risk event is very infrequent and unlikely to happen (i.e. at most once in ten years)	**Infrequent**	**2**
The risk event never happens	**Never**	**1**

Applying the matrix

The Branch uses the below risk rating table to determine the inherent/residual risk ratings based on the *red – amber - green (RAG)* matrix, where each risk is given a RAG score based on the likelihood versus the impact:

Impact score (inherent or residual risk score) x Likelihood score (weight) = Inherent or Residual Risk Rating

IMPACT

LIKELIHOOD

	1	2	3	4	5
1	LOW 1	LOW 2	LOW MEDIUM 3	LOW MEDIUM 4	MEDIUM 5
2	LOW 2	LOW MEDIUM 4	MEDIUM 6	MEDIUM 8	MEDIUM HIGH 10
3	LOW MEDIUM 3	MEDIUM 6	MEDIUM 9	MEDIUM HIGH 12	MEDIUM HIGH 15
4	LOW MEDIUM 4	MEDIUM 8	MEDIUM HIGH 12	MEDIUM HIGH 16	HIGH 20
5	MEDIUM 5	MEDIUM HIGH 10	MEDIUM HIGH 15	HIGH 20	HIGH 25

Risk rating key and steps to follow based on the achieved rating:

LOW 1-2 RISK IS ACCEPTABLE _____ OK TO PROCEED	LOW MEDIUM 3-4 RISK IS LOW AND ACCEPTABLE _____ TAKE MITIGATION EFFORTS	MEDIUM 5-9 RISK IS REASONABLY LOW _____ STRONGER MITIGATION EFFORTS ARE REQUIRED	MEDIUM HIGH 10-16 RISK IS GENERALLY UNACCEPTABLE _____ REQUIRE APPROVAL AND SEEK SUPPORT	HIGH 20-25 INTOLERABLE _____ PLACE ON HOLD, REQUIRE APPROVAL AND SEEK SUPPORT

1. **Low risk** – Where the Branch cannot eliminate a risk completely, the Branch aims to reduce it to the lowest risk rating possible. The ideal acceptable risk will be rated green which means that it is very unlikely to happen or is so minor that the effect of it occurring will not result in any major impact on the Branch. Thus, it is ok to proceed with the transaction without further approval, but these risks shall still be referenced on the assessment record to evidence identification and ensure future monitoring.
2. **Low medium** – In case of low medium rating the Branch deems the risks acceptable, but mitigation efforts must be taken nevertheless. MLRO approval is required.
3. **Medium** – Where pursuant to an assessment outcome the risk is reasonably low, the Branch must take stronger mitigation actions. The aim is to reduce all risks down to the lowest possible rating, however due to the nature or scope of the Branch's business, having medium or medium high risks is a factor of the services offered and it may be the case that they cannot be reduced further. Medium risks are still within the Branch's risk appetite. In such cases the Branch uses continuous monitoring and manages the risk as far as possible via control mechanisms in order to mitigate money laundering offences. MLRO approval is required.

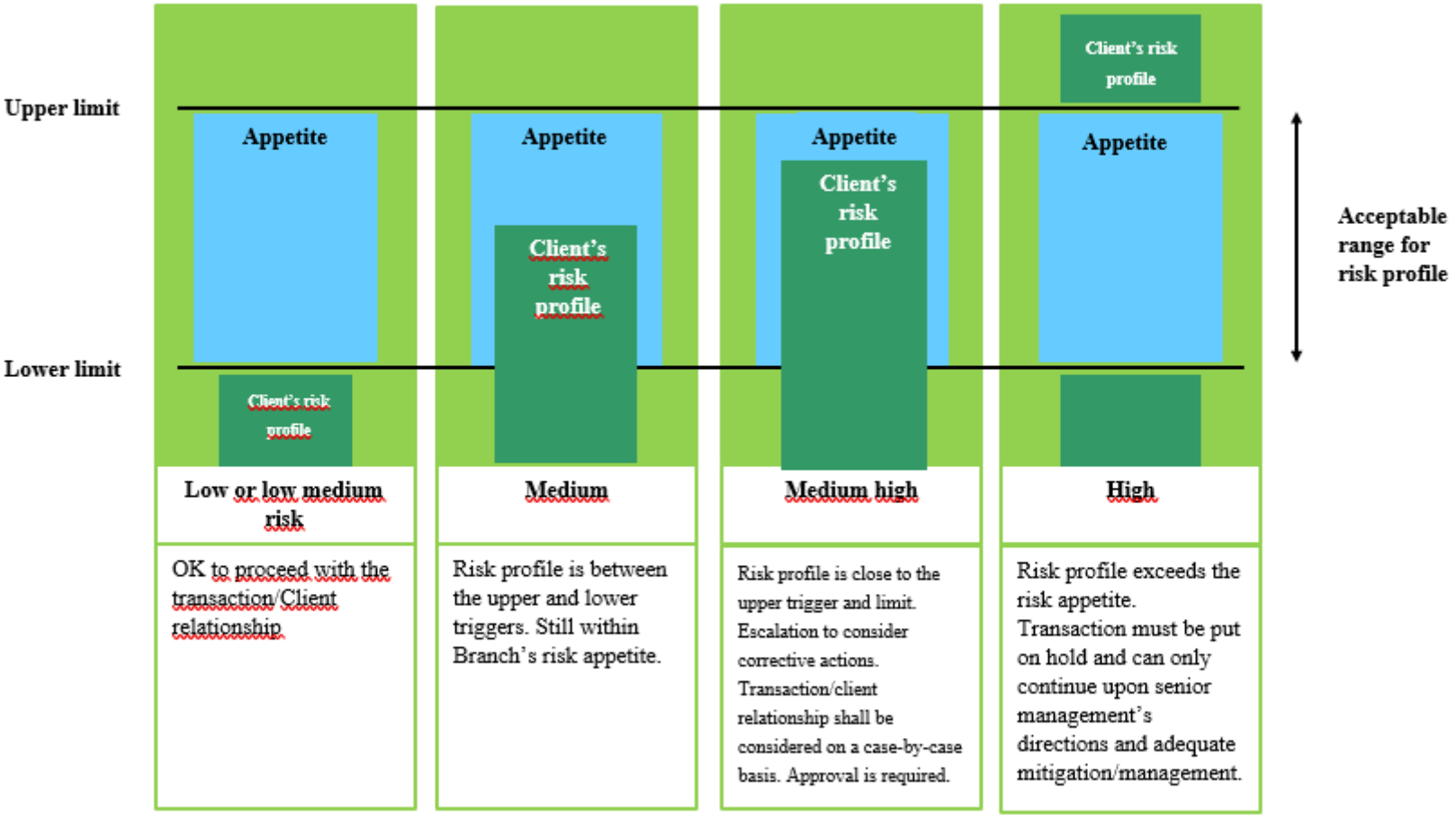
4. **Medium high** – Medium-high risk category represents risks that are generally unacceptable. Escalation to senior management, special approval and directions from senior management must be obtained and effective control mechanisms applied in order to reduce the risks to an acceptable level.
5. **High** – Where an assessment outcome indicates high risk rating, it means that either or both impact and likelihood scores are so high that there is an increased risk of being vulnerable to money laundering or terrorist financing. The Branch shall consider whether the risk can be eliminated through removal *(i.e. discarding a service in respect of that Client due to high risks or inability to effectively manage the money laundering risks)* or whether the risk can be lowered to an acceptable level. If the risk cannot be eliminated, the service/transaction is put on hold and strong controls and measures are implemented to reduce and manage the risk as far as possible (however the risk will still retain a "red" rating so that it is adequately monitored and reassessed accordingly). Escalation to senior management, special approval and directions from senior management must be obtained.

The Branch's risk appetite

When determining the risk appetite, the Branch considers:

- Regulatory risks
- Reputational risks
- Legal risks
- Financial risks.

Generally speaking, risks with medium risk rating are within the Branch's risk appetite. Medium high and high risks shall be considered on a case-by-case basis along with the possible further mitigation, risk management tools and the Client's overall risk profile. For example, if the Client's overall risk profile indicates a higher Client risk rating, but the other risk category ratings are within the Branch's appetite, enhanced due diligence is required to address the risk posed by the Client. If the risk can be managed effectively, senior management shall decide on moving the transaction/Client relationship forward.


Upper limit
Lower limit
Appetite
Client's risk profile
Low or low medium risk
OK to proceed with the transaction/Client relationship
Appetite
Client's risk profile
Medium
Risk profile is between the upper and lower triggers. Still within Branch's risk appetite.
Appetite
Client's risk profile
Medium high
Risk profile is close to the upper trigger and limit. Escalation to consider corrective actions. Transaction/client relationship shall be considered on a case-by-case basis. Approval is required.
Client's risk profile
Appetite
High
Risk profile exceeds the risk appetite. Transaction must be put on hold and can only continue upon senior management's directions and adequate mitigation/management.
Acceptable range for risk profile

Stage 6. Development & Implementation

Any controls, measures or systems identified in the previous stages that are *not already in place* are recorded, developed, sourced and/or implemented.
Other controls and measures identified during the previous stages *which are already in place* are reviewed for adequacy and effectiveness in accordance with the risk rating and desired outcome and improved/updated based on previous experience. The MLRO shall carry out these tasks and determine (in close co-operation with the director) further actions, remediation plans.

Where a service or business activity poses a high risk the Branch may place a temporary hold on such services/activities until the relevant controls have been developed, implemented and assessed.

Stage 7. Monitoring & Review

The Branch's procedures, controls and measures must be reviewed and reassessed annually to ensure they are still valid, effective and adequate.

The MLRO shall review the risk assessment procedures set out in this Manual and update the Manual in co-operation with and as approved by the managing director:

a) at least annually;
b) as required/if triggered (e.g. an external effect changes the nature of the risk or a new type of money laundering and terrorist financing risk or legislation arises, etc.);
c) on an ad hoc basis.

The completed risk assessment is also reviewed at least on an annual basis and each risk is reassessed to re-evaluate the risk rating, appropriateness and managing controls that have been put into place.

The Branch utilises suspected and/or submitted suspicious activity reports and internal reviews to evaluate the effectiveness and adequacy of the controls we have in place.

III. OTHER

III. 1. Branch wide assessment

In addition to the business line risk assessments, the Branch conducts an enterprise wide AML/CFT risk assessment every 2 years months. A more-frequent assessment is performed if new or emerging risks that significantly change the Branch's risk profile are identified.

III. 2. Record keeping obligations

The Branch makes and keeps records in relation to (a) its business relationship with each Client; and (b) each transaction that it conducts with or for the Client. The Branch will retain all records for at least ten (10) years in accordance with clause 7.1.2. of the AML/CFTR. Records are stored in accordance with applicable data protection laws. In order to ensure that all records can be retrieved without undue delay and provided to the supervisory authority if requested, the Branch will store the relevant data electronically in a highly protected manner.

APPENDIX 1

Example of residual risk rating calculation for CLIENT RISK category for the following business activity: "*Provision, formation and administration of trusts*"

Risk	Inherent risk score	Frequency (weighting)	Inherent risk rating as per RAG matrix	Control means and score	Residual risk	Residual risk rating as per RAG matrix	Frequency of ongoing monitoring	Type of CDD and level of approval
Client that is a legal person (trust, company or other legal arrangement) that has a complex business structure with little commercial justification, which obscures the identity of UBOs of the Client.	5	5 (risk is continuously outstanding)	25 (high)	Enhanced due diligence 3	5-3 = 2	10 (medium high)	Monthly monitoring	Enhanced CDD Approval of the managing director of the Branch

Client is engaged in a cash sensitive business.	3	4 (risk event may occur frequently)	12 (medium high)	1+1=2 Inquiring on the background and purpose of transactions that exceed predefined thresholds, to ensure alignment with Client's profiles (pre transaction checks) = 1 Continuous monitoring of transactions = 1	3-2 = 1	4 (low medium)	Annual monitoring	Simplified CDD MLRO approval

APPENDIX 2
Template

Risk	Inherent risk score	Frequency (weighting)	Inherent risk rating as per RAG matrix	Control means and score	Residual risk	Residual risk rating as per RAG matrix	Frequency of ongoing monitoring	Type of CDD and level of approval
[Please describe relevant risk]	*[Please attribute the relevant inherent risk score to the risk]*	*[Please determine the frequency of the risk to weigh and provide short explanation]*	*[Please apply score to RAG matrix and determine the inherent risk rating]*	*[Please determine the control measure and its relevant score]*	*[Please determine residual risk: inherent risk score-control means score]*	*[Please apply residual risk score and frequency to the RAG matrix and determine residual risk rating]*	*[Please determine the frequency for monitoring (please also consider the score within the risk category):* *<u>Low</u> or <u>Low medium</u> (lower score) risk category: every 6 months - annually* *<u>Low medium</u> (higher score), medium risk category:* *Every 3-6 months* *<u>Medium high</u> and <u>high</u> risk category: every 1 week – 3 months]*	*[Please determine the type of required client due diligence and the appropriate approval required for the one-off transaction/establishment of a relationship (please also consider clause V of the AML/CFT Policy and the score within the risk category):* *<u>Low</u> risk category:* - *Simplified CDD (please also see V.1. of the AML/CFT Policy) or CDD with reduced data content (in accordance with V.3. of the AML/CFT Policy)* - *no approval is required (unless*

								V.2.3. of the AML/CFT Policy so requires) *<u>Low Medium</u> or <u>Medium</u> risk category:* - *simplified or standard CDD* - *MLRO approval* *<u>Medium high</u> or <u>High</u> risk category:* - *enhanced CDD* - *approval of the managing director of the Branch is also needed]*