Julius Bär

Document title:	JBG-2003-00 Private Banking Client Acceptance Policy
Effective date:	05/05/2020
Version:	15.0
Approved by:	Oliver Bartholet, Raimund Röhrich
Author:	Patrick Regamey
General scope:	Legal Entities worldwide

	Significant regulated entities	All other Advisory Offices	Group WMCs	Other
Julius Baer Group	Bahamas Germany Guernsey Hong Kong India Luxembourg Monaco (Bank) Singapore Switzerland (Bank) U.A.E. UK	Austria Bahrain Chile Ireland Israel Lebanon Monaco JBWM Russia South Africa Spain Uruguay	Fransad Gestion GPS Brazil JB Fiduciaria (Milano) JBWM Nomura Kairos NSC Wergen & Partner	

SUMMARY

The Julius Baer Group (the Group) is committed to fighting money laundering (ML) and terrorist financing (TF) and to complying with all applicable Anti-Money Laundering (AML) and Counter Terrorism Financing (CTF) laws and regulations. The adoption of effective AML and CTF standards is an essential part of the Group's risk management framework, reducing the likelihood of becoming a victim of or being implicated by ML, TF and other unlawful activities.

This policy defines the principles, procedures and responsibilities for the acceptance, maintenance and closing of relationships with Private Banking (PB) clients. In addition, it covers the topics Know Your Client (KYC), Client Due Diligence, client risk categorization and periodic review for existing accounts. Institutional client relationships are generally subject to the stipulations of the D-1152-00 Client Acceptance and Maintenance Policy for Institutional Relationships. This policy adheres to the principles outlined in JBG-2000-00 Group Financial Crime Policy and is part of the Group's Financial Crime Compliance Policy Framework.

Key aspects of this policy

- Prohibited activities and relationships
- Group principles, procedures and responsibilities for client acceptance, maintenance and closing of relationship with Private Banking clients
- Definition of KYC principles and the components of Client Due Diligence e.g. identification & verification, screening, KYC profile, corroboration
- Handling of risk clients incl. risk categorization, risk criteria, approval process
- Review of existing relationships

Violation of this policy may result in disciplinary action.

1. PROHIBITED ACTIVITIES AND RELATIONSHIPS

The Group will not establish or maintain relationships with clients or other parties, which are prohibited by applicable laws and regulations, are inconsistent with the Group's Risk Tolerance Framework or by the Group's policies. These include, but are not limited to, the following prohibited activities and business relationships.

1.1. Prohibited Activities

The Group will not engage in the following activities:

- accept assets where the Group knows or must assume that they originate from a crime
- accept assets where the Group has indications of a non-tax compliant situation. For further details, reference is made to D-1133 Code of Conduct in Tax Matters
- assist their clients in acts aimed at deceiving authorities by means of incomplete or other misleading attestations
- assist in transferring unauthorised capital in the form of foreign exchange, banknotes or securities from a country that forbids or restricts such transfers abroad by its residents
- open anonymous accounts or accounts in fictitious names
- open accounts for legal entities with bearer shares
- offer services or products which are not in scope of the defined risk appetite. For further details, reference is made to the Group's Risk Tolerance Framework
- use the Group's own accounts or an employee account for the settlement of client transactions unless explicitly permitted by a Group policy (e.g. D-1112-00 Warehouse Policy)
- offer correspondent banking services to entities outside the Group. Banks and brokers as market counterparties are not classified as correspondent banking relationships. For details, reference is made to the D-1152-00 Client Acceptance and Maintenance Policy for Institutional Relationships
- assist in any activities which breach the international legislation related to combatting terrorism financing. For details, reference is made to the JBG-2007-00 Combatting Terrorism Financing Policy
- assist in any activities which breach the international legislation related to anti-bribery and corruption. For details, reference is made to the D-1023-00 Gifts and Entertainment & Anti-Corruption Policy.

1.2. Prohibited Relationships

Prohibited are relationships with certain persons or legal entities, where it is known or must be assumed that they:

- are unlicensed banks or financial intermediaries or money lenders
- are banks that have no physical presence in the country under the laws of which it is established (shell banks). Exceptions are entities, which are part of a financial group subject to effective consolidated supervision. For details, reference is made to the D-1152-00 Client Acceptance and Maintenance Policy for Institutional Relationships
- are correspondent banks providing services to shell banks
- are unlicensed and not appropriate supervised entities (under the laws and regulations of the corresponding country) involved in the operation of casinos, betting, bookmaking, private gambling/gaming club as well as other gambling related entities
- are involved in a criminal or terrorist organization, or support such an organization
- are involved in an extreme political or religious organization, or support such an organization[1]
- are outside the Group's defined risk appetite. For further details, reference is made to the Group's Risk Tolerance Framework
- are classified by the Group or one of its legal entities as unwanted clients/business relationships
- support or carry out unlicensed money remittance or value transfer business. This covers unlicensed or unregulated entities and the activities, assets and income derived from the money remittance business. This is especially valid for informal money transfer networks, such as "hawala", "hundi", "chop" and for those engaged bulk cash smuggling
- are prohibited under applicable sanctions and embargoes laws or regulations, or as defined in the D-1079-00 International Sanctions and Embargos and accompanying standards.

[1] This can be generally defined as all kind of persons or organizations whose views, objectives and activities are considered extreme and intolerant towards third parties and represent an unacceptable legal and / or reputational risk to the bank. "Extreme" in this sense means the pursuance of political or religious ideology to its limits without regard to its impacts with the intention to confront and eliminate the opposition.

2. KYC PRINCIPLES

KYC is the process of establishing comprehensive profiles of the Group's clients[2] and verifying its content through reliable sources. It is governed by principles that form the basis of the Group's commitment to KYC standards as required by law and as applied by the community of international Private Banks. Through the application of these principles, the Group also ensures a holistic approach for Client Due Diligence (CDD). The adoption of effective KYC standards is therefore an essential part of the Group's risk management framework, reducing the likelihood of becoming a victim to or being implicated by ML, TF and other unlawful activities. The KYC principles are explained below as follows:

2.1. Principle 1: Risk Based Approach

The concept of a risk-based approach is one of the key principles of sound risk management practices in the area of financial crime risks. Following a risk based approach implies that CDD measures and controls are commensurate with the actual nature and level of the client risk identified. Thus, for relationships with in-creased risk, the corresponding measures have to be more rigorous and granular (Enhanced Due Diligence) than relationships without increased risk (Standard Due Diligence). Refer to section 3.1 for further details on CDD.

The extent of the information as well as any related supporting documentation must therefore reflect the specific risks as determined by client risk factors, the (economic) background, purpose and intended nature of the business relationship and any other information having an impact on the overall client risk.

2.2. Principle 2: Accuracy and Completeness of Information

KYC profile information obtained must be accurate, complete, up-to-date and comprehensive. KYC profiles must reflect the factual situation and circumstances of the client. The storyline provided must therefore contain sufficient information about any potential underlying reputational or Financial Crime risks of a client. If the quality of the storyline does not provide the appropriate level of detail, additional information has to be obtained from the client or their representatives and/or independent, reliable sources.

Furthermore, the information captured in the KYC profile is to be recorded and documented in such a manner that it is fully understandable for third parties. The documentation of hyperlinks and the storage of password-protected documents are not allowed. The relationship manager (RM) compiles the KYC profile information in the appropriate client relationship management system.

2.3. Principle 3: Information from Independent Sources and Plausibility

It is good practice to check information used to support KYC profiles for its reliability. When relying on supporting documents, a bank should be aware that the most reliable documents are those most difficult to obtain illicitly or to counterfeit (reference

[2] The term "client" refers to the person who has a business relationship with the Bank (Contracting Party), also referred to as Account Holder, and/or the beneficial owner(s), as the case may be.

is made to section 5 for corroboration requirements and Appendix 5). These may include government-issued documents, reports from independent (public) sources or other reliable sources as well as observations made by the RM himself/herself, e.g. visit to the client's premises. If there are indications that point to potential partiality, bias or undue influence of sources, appropriate clarifications must be provided in order to determine the reliability of the information.

Due care has to be taken while reviewing information received from the client. Client information shall always be treated with an adequate level of scrutiny and checked by the responsible RM with regard to its plausibility. This equally applies where external asset managers (EAM) or external financial advisers (EFA), have submitted the respective information.

At account opening and periodic reviews or reviews triggered by a risk event, all available information must be assessed holistically. If there are elements in the client story that do not fit together, or are not sufficiently explained (e.g. very generic explanations), or there are documents that seem not to support elements of the client story, or the KYC profile in its entirety does not appear reasonable or plausible, the veracity of information has to be challenged. The RM must contact the client or the EAM/EFA in such cases and request clarifications (including supporting documents) to clear any contradictions.

2.4. Principle 4: Maintaining Updated KYC Information

The KYC profile information must be kept up-to-date. It is the responsibility of the RM to maintain the KYC profile information up-to-date. The RM ensures that relevant updates are initiated and reflected in the KYC profile on a timely basis during the entire course of the account relationship. Any information relevant to the KYC profile, which comes to the attention of the RM, must be made available in the appropriate client relationship management system as soon as reasonably possible. Where necessary, the RM has to support the recorded information with relevant documentation.

Where the RM is not certain or has reasonable doubts about whether the KYC Profile is still up-to-date, he or she has to actively clarify if the information on file is still valid.

In case of trigger events (e.g. changes concerning the domicile or the professional activities) with material changes to the client's risk profile (e.g. new risk factors) or concerns noted on the client's KYC profile (e.g. new information does not appear reasonable or plausible), the RM has to escalate this to his/her superior and local Compliance for review and assessment as soon as he is aware of the change.

Periodic risk reviews of the client relationship following the same principles as outlined in this policy have to be conducted by the RM at regular intervals depending on the underlying risk identified for the client (reference is made to section 7).

2.5. Principle 5: Grandfathering

Within the applicable laws and regulations, the grandfathering principle allows KYC profiles that were approved before the implementation of a new rule concerning KYC standards and KYC questionnaires to continue for a set period of time, while the new rule does only apply to all new account openings.

Depending on the significance of the changes based upon the new rule, an impact analysis shall determine whether the changes apply in retrospective. Minor changes do not require an impact analysis and thus such changes are deemed "grandfathered" without retrospective effect. Such an impact analysis is assessed by the local Head Compliance, and, where necessary, presented to the Local/Regional CRO and Group Head Financial Crime Compliance for final decision on how to proceed.

3. RISK CRITERIA AND CLIENT DUE DILIGENCE

The Group identifies and determines the risk criteria to be used for the risk categorization of a relationship. The Group distinguishes between standard risk client relationships and risk client relationships. The following criteria lead to a categorization as risk client relationship:

- Politically exposed person (PEP)
- Large clients
- Sensitive industry
- Risk country
- Commercial accounts
- Complex ownership structure
- Other risk criteria

Relationships with standard risk are all relationships, which do not fulfil any of the risk criteria above.

The risk categorization allows the Group to assess and classify the risk of all new and existing clients to determine the corresponding level of CDD required. The presence of risk criteria may require an assessment whether the client meets the criteria of a prohibited activity or relationship (reference is made to section 1). Such cases must be escalated by the Front Office[3] to local Compliance.

The risk categorization of a relationship is triggered by the:

- contracting party/account holder,
- beneficial owner or equivalent roles (reference is made to section 4.1.5.1), or
- holder of a power of attorney and/or authorized signatory (solely relevant regarding the risk criteria PEP and risk country).

[3] "Front Office" refers to relationship managers, assistant relationship managers, line managers of relationship managers, account managers, or other first line of defense employees.

3.1. Client Due Diligence

CDD is the process where relevant information and related supporting documentation about the client is collected, and ongoing monitoring is performed on the client to evaluate for any potential ML/TF risks posed by the client.

All clients and their account relationships are subject to CDD measures before starting a relationship and throughout the lifecycle of the relationship, e.g. periodic reviews, trigger events due to changes in the client profile or risk factors. CDD measures comprise:

- Obtaining information and documents on the client's KYC profile including identification and verification measures, and understanding the purpose and intended nature of the business relationship
- Name screening and media searches
- Conducting ongoing due diligence on the relationship and transaction monitoring to ensure transactions conducted are consistent with the client's profile (reference is made to policy JBG-2001-00 Global Anti-Money Laundering Monitoring Policy).

The CDD process consists of Standard Due Diligence (SDD) and Enhanced Due Diligence (EDD). For further information on the level of due diligence applied, reference is made to the sections 3.1.1 and 3.1.2 and Appendix 4.

For the risk classification of Institutional Relationships, reference is made to D-1152-00 Client Acceptance and Maintenance Policy for Institutional Relationships.

3.1.1. Standard Due Diligence

SDD is applied to all cases where EDD is not applied and the risk of a relationship is classified as standard. When reviewing a client under the provisions of SDD, risks may become apparent which require EDD to be applied in order to understand and subsequently manage these risks appropriately.

3.1.2. Enhanced Due Diligence

EDD is applicable to clients who fulfil one or more of the outlined risk criteria in this policy and are identified as relationships representing increased risk. EDD may encompass more detailed, extensive KYC profile information, supporting documents and/or higher frequency of reviews compared to SDD, and in particular, a more comprehensive assessment of the risks involved.

The extent and nature of EDD measures applied may vary depending upon the nature of the related risk factors. EDD information can be obtained from multiple sources, including publicly available information, such as property, land and company registers, press reports, reports provided by third party service providers, commercial databases, information from other banking relationship (such as a financial institution the client currently holds an account with), discussions with the client etc. It is important that, wherever possible, multiple sources of information be used when conducting EDD to corroborate such information.

3.2. Risk Criteria

3.2.1. Politically Exposed Person

Relationships with PEPs are classified as risk relationship.

3.2.1.1. Definition

PEPs are defined as natural persons who are or have been entrusted with a prominent public function including close family members and close associates of such natural persons and may have substantial authority over policy, operations or the use or allocation of government-owned resources. In particular, the following non-exhaustive positions meet the criteria of a prominent public function:

- Heads of state or of government of any country or state or sub-section of such a government and their deputies (e.g. royal families with executive power, ministers, governors of states or provinces)
- Senior politicians at national level (e.g. members of parliament)
- Senior government, judicial, military or party officials on the national level (e.g. secretaries of state, high-ranking officials in the administration, judges of the supreme court, federal prosecutors, high-ranking members of military branches, police forces and secret services, members of governing bodies of national political parties (e.g. president or general secretaries), high-level or influential representatives of religious organizations if their function is linked to government, political, judicial, military responsibilities)
- State-owned/controlled (i.e. 50% capital and/or voting rights) entities of national importance and/or senior executives (e.g. directors, executive staff) of such enterprises (e.g. Chief Executive Officer (CEO) of a state-owned oil company)
- Persons who have a prominent function in an intergovernmental organization, i.e. members of senior management or individuals who have been entrusted with equivalent functions, such as directors, deputy directors and members of the board or equivalent functions (e.g. Representatives of Organization for Economic and Cooperation and Development or United Nations (UN) General Assembly members, general directors of an UN Specialized Agency)
- Persons who have a prominent function in an international sports federation (e.g. members of the International Olympic Committee, president and executive members of the Fédération Internationale de Football Association or Fédération Internationale de l'Automobile).

As **close family members** are considered:

- Close family (e.g. spouses, parents, children, grandchildren, siblings)
- Other close relatives (e.g. nephew/niece, uncle/aunt)
- Close family members through marriage (e.g. brother/sister-in-law, father/mother in-law).

Close associates are all individuals or legal entities who have recognisably close connections to a PEP for social or professional reasons but do not fall into the category of close family members. In particular, the following connections are considered close:

- personal advisors (e.g. financial advisors or persons acting in a financial fiduciary capacity)
- Operationally active companies owned and/or controlled by a PEP (e.g. PEP is not acting in his/her official capacity, has independent decision-making powers within a significant area of responsibility or companies where a government minister is CEO or similar whose activity is not related to his/her post) and/or where the PEP has a considerable financial interest (e.g. the PEP holding at least 25 % voting and/or capital rights in the company).

The social, economic, and cultural context may play a role in determining the closeness of a relationship to a PEP.

3.2.1.2. Responsibilities concerning the detection of PEPs

The Group uses tools and databases to screen prospective and existing relationships for PEP connections. In addition, the Group relies on the due diligence of the RM, who must escalate it to his/her superior and local Compliance whenever he detects a potential PEP nexus.

Local Compliance acts as point of entry for any inquiries or advice in connection with relationships associated with PEPs and reports any new PEP relationship timely to the Group PEP Desk (reference is made to section 3.3.1).

It is important to note that the process of assessing whether a client is a PEP cannot be entirely standardized and some degree of judgement has to be exercised, always considering the facts of each case and the unique profile of each client. A proper documentation of the assessment by local Compliance is required if despite certain indications that point to a potential PEP status, a client is not classified as PEP.

3.2.1.3. Responsibilities of the Group PEP Desk

The Group PEP Desk answers questions related to PEPs and PEP relationships (e.g. if a relationship for the PEP in question already exists or if a previous request has been rejected). The Group PEP Desk also manages and maintains a database containing all known PEP relationships within the Group. These relationships are evaluated by the Group PEP Desk on an on-going basis according to the risks associated therewith.

The Group PEP Desk follows general political developments in the markets and gathers and evaluates information on PEPs. Furthermore, the Group PEP Desk acts as coordinator on all PEP related matters (e.g. PEP designations) with local Compliance and has the ultimate authority in determining any PEP status.

3.2.1.4. Duration of PEP Attribute

Should a PEP lose his/her function, local Compliance and the Group PEP Desk must be consulted as to whether the PEP flag still has to be set (for new relationships) respectively may be removed (for existing relationships). The risk associated with holding prominent public functions is not necessarily diminished as soon as the PEP has stepped down. While the time elapsed since stepping down from a PEP function is a relevant factor to consider, a holistic approach shall be taken to consider the level of PEP risk such persons may continue to exercise. This must be assessed on a case-by-case basis using a risk-based approach. Risk factors to consider include the level of (informal) influence that the individual could still exercise, the seniority and length of the position that the individual previously held as a PEP, whether the individual's previous and current function are linked in any way and the level of inherent corruption risk in their country of political exposure. The assessment must be documented. In case of a Cross Unit Relationship (CUR) set-up, Compliance at the Booking Centre, when removing the PEP classification of a relationship, must inform Compliance of the Advisory Office or the Group Wealth Management Company (thereafter collectively referred to as Advisory Location) and the Account Manager in the Booking Centre accordingly. The same applies in cases where Compliance of an Advisory Location removes the PEP attribute of a relationship.

In any case, removing a PEP classification may not be considered earlier than 18 months after the PEP has lost his/her public function.

3.2.2. Large Clients

Clients who intend to place or have effectively placed assets (Assets under Management) of an overall size exceeding CHF 50 million or equivalent are considered large clients and classified as risk relationships. This rule applies also for clients who plan to place or have effectively placed assets in this amount on a consolidated basis, i.e. multiple accounts with identical beneficial ownership status (Booking Centre view).

3.2.3. Sensitive Industries

Clients with a substantial connection to one of the following sensitive industries are classified as risk relationships:

- Weapons, armament manufacturers, traders and intermediaries
- Casinos, gambling and other connected industries
- Charities, religious, political and other non-profit organisations
- Precious stones (e.g. diamonds) and metal traders, jewellery dealers
- Tobacco traders

- Arts and antique dealing
- Adult entertainment industry
- Regulated money transfer agents
- Non-professional regulated foreign exchange dealers
- Professional money changers in the non-bank sector (regulated and non-regulated).

For definitions and guidelines on the application of sensitive industries, reference is made to Appendix 1.

The responsible RM must assess in each case if a relevant substantial connection exists on a consolidated basis across all sensitive industries. A substantial connection may exist in one the following cases:

Contracting Partner / Beneficial Owner	Cases of substantial connection
Legal Entities	• Operating legal entities directly engaged in a sensitive industry (including one-man companies, agents, etc.) • Operating legal entities or holding companies achieving 25 % of its overall income from a sensitive industry. Suppliers or providers of goods or services to individuals or legal entities engaged in a sensitive industry are excluded provided that the good or services themselves are not sensitive • Charities related to a risk country as set out in Appendix 2.
Individuals[4]	• Major investments or ownership rights (shareholders 25 % or more of voting or capital rights) of a legal entity engaged in a sensitive industry • Business activity(ies) or Source of Wealth contribution of 25 % or more related to a sensitive industry • Members of a senior executive of a legal entity engaged in a sensitive industry. All other employees of such legal entities are excluded.

Local Compliance acts as point of entry for any inquiries or advice in connection with relationships associated with a sensitive industry.

3.2.4. Risk Country

Clients associated with a risk country are categorized as risk relationship. For a detailed list of the risk countries, reference is made to Appendix 2. The following factors lead to a risk country categorization:

- Nationality
- Domicile / Incorporation
- Business activity(ies) or Source of Wealth (SoW) accumulation with substantial connection[5] to a risk country.

Should there be more than one country involved, the key risk country (usually the one with the highest risk score/factor) must be identified (e.g. the account holder is

[4] Applies also to a trust, foundation, domiciliary company or other legal vehicle beneficially owned by an individual.
[5] A substantial connection is assumed if more than 25 % of the business activities or SoW accumulation takes/took place in a risk country.

domiciled in Cyprus, the ultimate beneficial owner is domiciled in Russia, the key risk country would therefore be Russia).

3.2.5. Commercial Accounts

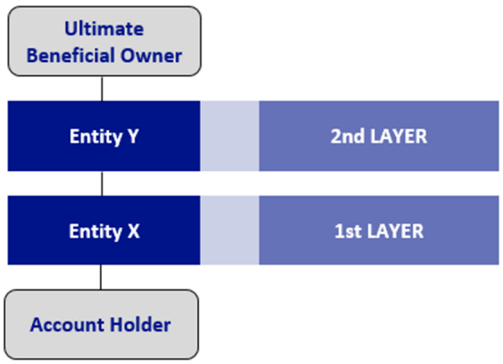
Commercial accounts are classified as risk relationships. The Group defines commercial accounts by applying a qualitative element, i.e. the definition of what constitutes a commercial transaction, and a quantitative element that sets out various thresholds (e.g. number of transactions, amounts transferred). The qualitative elements sets out that a commercial transaction is a transaction that does not serve the investment of private wealth of a PB client and that involves regular payments to/from third parties with which the client is in a profit-oriented commercial relationship (e.g. buying/selling goods, providing services, leases).

If an account has been flagged as commercial, the KYC profile must meet additional requirements such as documenting the client's reasons and justification for conducting commercial activities through a private banking account instead of a corporate or institutional account, expected transaction activities, counterparties and their relationship with the client. For examples of the qualitative element and the details of the quantitative element of commercial accounts and the related enhanced procedures, reference is made to Appendix 3.

3.2.6. Complex Ownership Structures

Complex ownership structures are classified as risk relationships. In general, a complex structure is defined as an ownership structure involving two or more vertical layers of ownership. The account holder and the ultimate beneficial owner (UBO[6]) are not counted as a layer[7]. A layer is defined as one entity (or unincorporated structure) owned by a next layer.

Example of a complex structure:



[6] The term UBO is commonly used in the context of complex ownership structures where the UBO owns or controls a legal entity (or an unincorporated vehicle) through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that entity. The UBO is always a natural person. For further details, reference is made to section 4.1.5.1.
[7] The nominee shareholders of a domiciliary company underlying a trust are exempted i.e. do not count as an intermediate layer.

The RM needs to provide further information for complex structures involving two or more layers of ownership based upon the explanations and documents provided by the client:

- Client's rationale for using a complex structure
- Ownership / control structure diagram providing information on ownership / control for each layer and
- Documents corroborating the control and ownership layers of which the account holder is part of (where applicable).

A legal opinion from the client's advisers (e.g. reputable legal, tax or wealth planners) needs to be requested where the rationale for choosing a complex ownership structure is not clear, does not appear to be legitimate or the ownership structure itself appears to be excessively complex or seems illegitimate. Irrespective of the client's rationale for choosing a complex ownership structure, local Compliance may request identification and verification documents (corporate documents) for the intermediate layers.

Further, domiciliary companies with no or one intermediate layer classify as a complex structure if they meet two of the following three criteria cumulatively:

- There is a nominee shareholder involved holding more than 1% of the shares[8]
- The domiciliary company is domiciled in an intransparent jurisdiction according to the Non-Reportable / Tax Haven Jurisdictions List
- Assets are placed for a short-term only[9].

The RM needs to provide the client's rationale for the use of nominee shareholders and/or for the short-term asset placement.

3.2.7. Other Risk Criteria

The RM or local Compliance may classify a relationship as risk relationship based upon other risk criteria that potentially represent a financial crime risk or other significant reputational risk to the Group.

3.3. Account Opening Approvals

3.3.1. Required Approvals

The approvals of a relationship follow a predefined process. Therefore, risk relationships have to fulfil higher requirements than relationships with standard risks, e.g. additional approvals within the onboarding process are required.

[8] Nominee shareholders of a Domiciliary Company underlying a trust are exempted.
[9] Short-term asset placement is defined as: in- and outflow of assets within one month if the outflow is equal to or higher than 90% of the assets that have previously been placed with the Group. Cases where the outlined criterion is not met but the primary purpose of the account (holding of assets) is diluted by frequent shifts on the account (e.g. pass-through transactions), may still qualify as short-term asset placement. Any such observations have to be escalated by the RM and/or superior to local Compliance who has to holistically assess whether the transactional behavior/overall account purpose must be assessed as short-term asset placement.

The following table outlines the required approvals to open a relationship:

PEP[10]	**Large Clients/ Sensitive Industry/ Commercial Accounts/ Complex Ownership Structure**	**Risk Country**	**Standard Risk**
Responsibility: Performance and documentation of EDD: • RM **Review & Approvals:** • Superior • Risk Country Market Head if risk country involved[11] • Local Compliance • Region Head[12] **Head Office** • Group PEP Desk • Group Chief Risk Officer (CRO)	**Responsibility:** Performance and documentation of EDD: • RM **Review & Approvals:** • Superior • Risk Country Market Head if risk country involved[11] • Local Compliance • Region Head[12]	**Responsibility:** Performance and documentation of EDD: • RM **Review & Approvals:** • Superior • Risk Country Market Head[11] • Local Compliance	**Responsibility:** Performance and documentation of EDD: • RM **Review & Approvals:** • Superior • Local Compliance[13]

For relationships that fulfil the requirements of more than one risk category, the strictest approval requirements apply. All approvals must be appropriately documented, either in electronic or physical form.

Principles of adequate segregation of duties to minimize potential conflicts of interest shall be observed for approvals. RMs shall not be approving their own accounts in any superior role and/or management capacity (including Risk Country Market Head role). Delegation of approvals shall be to persons independent of the client coverage RM team. In line with the principles of adequate segregation, it has to be ensured that a person does not provide multiple approvals for a relationship (e.g. once in the function as Risk Country Market Head and once as delegate of the Region Head). Where the size of the location does not allow for full implementation of the principles of adequate segregation, the approval framework must be reviewed with and approved by the Group Head Financial Crime Compliance.

As part of the onboarding of new relationships and/or the ongoing monitoring of relationships, local Compliance may impose Compliance conditions (conditions). A condition is every additional requirement that goes beyond the scope of the existing policy framework in order to ensure that the risks present in a relationship are (and will remain) within the Group's risk appetite. Such conditions must be agreed in writing between local Compliance and the Front Office or decided by the local CRO. The RM is responsible to fulfil the conditions within the required timelines and submit the

[10] The outlined approval process applies to relationships which fulfil the requirements of the global PEP definition (reference is made to section 3.2.1.1). Regarding the approval process for relationships that correspond to a local PEP definition, which is going beyond the outlined global PEP definition, reference is made to section 3.3.3.6.
[11] If there are multiple risk countries involved, Risk Country Market Head approval for the identified key risk country is required (reference is made to section 3.2.4).
[12] Outside of Switzerland, where an account is managed by an RM who reports to a Region Head outside of the jurisdiction where the assets are booked, the approval of the Region Head responsible for the RM is sufficient.
[13] Local Compliance may apply a sample-based approach. Details of the sample-based approach must be defined in a local policy.

relevant documents and information to his/her superior and local Compliance. Local Compliance, as second line of defence, performs additional controls (i.e. timely and appropriate fulfilment of the conditions).

In case of CUR set-ups, Compliance at the Booking Centre must inform Compliance at the Advisory Location and the Account Manager in the Booking Centre accordingly. However, also in a CUR set-up, the RM remains responsible to fulfil the condition within the required timelines and submit the relevant documents and information to his/her superior and local Compliance. Compliance in the Booking Centre is responsible to perform additional controls (i.e. timely and appropriate fulfilment of the conditions), with the assistance of Compliance in the Advisory Location, if deemed necessary.

3.3.2. Escalation Procedure in Case of Disagreements between Front Office and Local Compliance

The decision with regard to the account opening of relationships shall be reached with unanimity between Front Office/Risk Country Market Head and local Compliance. Where such agreements between Front Office/Risk Country Market Head and local Compliance cannot be reached, the case escalation shall follow the procedures outlined below:

- Escalation to the local Client Review Committee (CRC) if such committee has been established. For further details on binding rules for the CRC, reference is made to G-1026-02 Global Terms of Reference – Client Review Committee
- In the absence of a local CRC, escalation to the Location Head and Local CRO
- In the event that no agreement can be reached at the local level, the case may be escalated to the Region Head and Group CRO for final decision.

3.3.3. Responsibilities of the Approvers

3.3.3.1. Relationship Manager

Before a relationship is established, the RM performs SDD or EDD (reference is made to sections 1 to 5). The RM ensures that the relationships are flagged accordingly and contacts local Compliance for additional due diligence measures where necessary. The RM has to assess if he is comfortable with the overall risk represented in the relationship and in case of a negative assessment, forego the account opening.

3.3.3.2. Superior

The superior reviews and approves in a second step each relationship. He ensures that the requirements of SDD or EDD are met (reference is made to sections 1 to and 5).

3.3.3.3. Risk Country Market Head

Relationships associated with a risk country (i.e. nationality, domicile / incorporation and/or business with substantial connection to such a country) must be additionally reviewed and approved by the Risk Country Market Head responsible for the country in question or a designated deputy responsible. Where the Risk Country Market Head is located within a different location to where the assets will be booked, it must be ensured that the approval process is in line with local banking secrecy/professional secrecy and data protection regulations.

Clients with a second nationality in the jurisdictions Aruba, Belize, Bonaire/Saint Estatius/Saba, Curaçao, Dominica, Dominican Republic and St. Kitts and Nevis, are exempted from the Risk Country Market Head approval for the second nationality.

3.3.3.4. Local Compliance

Local Compliance conducts a completeness and plausibility check of the information and required supporting information/documentation (as outlined in sections 4.2 to 4.8 and 5). Where required, local Compliance will liaise with the RM to request additional information/documentation. Local Compliance ensures that all relevant risks are adequately addressed and if needed escalated to the relevant stakeholders. Local Compliance ensures that the results of its review is documented appropriately.

3.3.3.5. Region Head

The Region Head reviews and approves all risk relationships. The Region Head may delegate his/her duty to review and approve the acceptance of risk relationships to a direct report with the exception of PEP relationships.

3.3.3.6. Group PEP Desk

For relationships associated with a PEP booked in Switzerland, the Group PEP Desk performs the function of local Compliance outlined in section 3.3.3.4.

In cases of relationships associated with a PEP booked outside of Switzerland, the case is forwarded by local Compliance to the Group PEP Desk for review and approval.

Relationships that correspond to a local PEP definition based on applicable local laws and regulations, which is going further than the outlined global PEP definition (reference is made to section 3.2.1.1), have to be reviewed and approved by the RM, his/her superior, Risk Country Market Head if a risk country involved, Local Compliance and Region Head (as outlined in the sections 3.3.3.1 to 3.3.3.5), and to be reported timely to the Group PEP Desk.

3.3.3.7. Group CRO

The Group CRO is the final approver for risk relationships associated with PEP or for cases where no agreement can be reached at the local level. The decision by the Group CRO cannot be overruled by business management.

3.3.4. Risk Category Change of Existing Relationships

The monitoring and maintaining of relationships is the responsibility of the RM and his/her superior (reference is made to JBG-2001-00 Global Anti-Money Laundering Monitoring Policy). The RM has to ensure that the documented client information is complete and up-to-date. Changes of client information may lead to the following impact on the risk categorization of an existing relationship:

- Change of the risk categorization from standard risk to risk relationship (Upgrade)
- Change of the risk categorization from risk relationship to standard risk (Declassification)
- Additional risk criteria without change of risk categorization.

An upgrade is typically required when at least one risk criterion according to section 3.2 is newly identified for a standard risk relationship. A declassification may be appropriate if a risk criterion for a risk relationship ceases to exist and there are no other risk criteria present.

3.3.4.1. Upgrade of Risk Category

If a relationship becomes a risk relationship, the RM has to timely inform his/her superior and local Compliance. Local Compliance defines the scope and depth of the review to be performed by the RM. In any case, the RM must assess the change of risk and whether he feels comfortable with the newly identified risk criterion and has to complete the approval process according to section 3.3.1. Any Compliance assessment conducted must be documented accordingly.

3.3.4.2. Declassification of Risk Category ("Cooling-off period")

The risk criteria of an existing relationship may disappear or diminish over time. To declassify an existing risk relationship, a minimum period of at least one year since the removal of the risk criteria should usually elapse. A longer cooling-off period may be appropriate where the influence of the risk criteria remain.

In cases where a risk country client changes the domicile to a non-risk country, no cooling-off period is required.

Once the cooling-off period has elapsed, the RM may apply for the declassification of the relationship to his/her superior and local Compliance. It is then up to local Compliance to decide whether a review should be initiated or not and (if applicable) to define the scope and depth of the review. Any Compliance assessment conducted must be documented accordingly.

For the process regarding relationships associated with PEP, reference is made to section 3.2.1.4.

3.3.4.3. Additional Risk Criteria but no Change of Risk Categorization

If for a risk relationship an additional risk criteria is newly identified, the RM must assess whether he feels comfortable with the newly identified risk criterion and has to inform his/her superior and local Compliance. It is then up to local Compliance to

decide whether a review should be initiated or not and (if applicable) to define the scope and depth of the review. However, the RM must obtain additional approvals where required (reference is made to section 3.3.1). Any Compliance assessment conducted must be documented accordingly.

4. COMPONENTS OF THE CDD AND KYC PROFILE

The RM must document the KYC information in the client profile. It contains relevant information of the personal and economic background of the client. Other related parties connected to the account, e.g. power of attorney, authorized signatory, must also be considered in the KYC profile. The scope of information in the KYC profile shall correspond to the role exercised by these partners respectively. All client relationships require a client profile, irrespective of the amount of assets deposited or the risk profile respectively. The client profiles must contain the following:

4.1. Identification & Verification

4.1.1. Identification & Verification of Identity Principles

4.1.1.1. Necessity of Identifying and Verifying the Identity of Clients

The requirements as outlined in the below sections must be followed when the Group

- establishes relationships with any client regardless of whether any assets are booked with the Group or not, or
- has doubts about the veracity or adequacy of any information or documents previously obtained.

The Group is not allowed to provide any banking services such as cash transactions (e.g. currency exchange) or wire transfers without establishing a relationship with clients demanding such services.

4.1.1.2. How to Identify and Verify the Identity of Clients

The Group has to obtain the original or a certified true copy of identification document from the client. The copy must be of good quality. A copy of an identification document may be certified to be a true copy by any of the below options:

- A Front Office employee of the Group
- A bank or another financial institution recognized for this purpose
- An External Asset Manager/External Financial Adviser
- A notary or another official body that customarily issues such authentications.

4.1.1.3. Face-to-face Verification of the Clients Identity

A Front Office employee of the Group has to verify the identity of a natural person within a face-to-face meeting using a certified true copy of an official identification document with a photograph (e.g. passport).

In such cases, the Front Office employee has to copy the identification document and certify on the photocopy that the original identification document has been reviewed. Signature of the Front Office employee and the date of verification must be included on the copy.

4.1.1.4. Delegation of Identification and Verification Processes

The delegation of identification and verification processes to an External Asset Manager/External Financial Adviser (herein after referred to as delegate) may only be approved if the following requirements are cumulatively met:

- The Group has carefully selected the delegate
- There is a written agreement in place between the Group and the delegate whereby the Group has given such persons or companies appropriate instructions regarding their responsibilities
- The Group controls whether the delegate adheres to his responsibilities according to the agreement.

Despite the delegation, the responsibility for ensuring the correctness of the identification and verification process remains with the Group. For further details, reference is made to D-1059-00 Business Relationship with External Asset Managers.

4.1.1.5. Establishing a Relationship by Correspondence

Where a relationship is established by correspondence, the Group must verify the identity of the account holder by obtaining a copy of an identification document certified by a notary or another official body that customarily issues such authentications. In addition, the Group shall confirm the account holder's address either by postal delivery or by another equivalent method (e.g. official confirmation of residence). A delegate can only verify the account holder's identity in a face-to-face meeting but not via correspondence.

4.1.1.6. Timing of Identification and Verification Processes

All documents required to identify and verify the identity of clients as outlined in this policy must be duly and completely presented before an account can be used. An account is deemed usable from the point at which in- and outflows can be made to it. In exceptional cases, an account may be used where only minor information and/or documents are missing or where particular documents have not been provided in the appropriate form. Compliance must assess each case using a risk-based approach, verifying in particular whether the exception is necessary in order to not disrupt the ordinary course of business.

The missing information and/or documents must be made available by the Front Office as soon as possible, at the latest within 30 calendar days after the account can be used. If not provided within this timeframe, the account will be blocked for all transactions and Compliance must decide whether the missing information and/or documentation will likely be made available without further delay or whether the business relationship must be closed in a timely manner.

4.1.2. Identification and Verification of the Identity of Natural Persons as Account Holder

For natural persons who wish to enter into a relationship with the Group, at least the following information must be obtained:

- Last name(s)
- First name(s)
- Date of birth
- Nationality/-ies
- Residential address.

In general, a c/o-address or a P.O. Box address as residential address is not acceptable. The Group may accept P.O. Box addresses for natural persons of certain countries where it is clearly established that P.O. Box addresses are common residential addresses.

4.1.3. Identification and Verification of the Identity of Legal Persons or Legal Arrangements as Account Holders

For legal persons or legal arrangements who wish to enter into a relationship with the Group, at least the following information must be obtained:

- Full name
- Incorporation or business registration number
- Registered or business address
- Date of establishment, incorporation or registration
- Place of incorporation or registration
- Legal form.

Where the account holder is a legal person or a legal arrangement, the Group shall, apart from identifying the account holder, also identify the constitution and powers that regulate and bind the legal person or legal arrangement by means of a register extract issued by the registrar or a written extract from a database maintained by the registry or by using other reliable, independent source data, documents or information.

4.1.4. Identity of Persons Appointed to act on a Client's Behalf

Where the account holder appoints one or more persons to act on his behalf in establishing a relationship, the Group has to check the identity of the persons that act on behalf of the client. This can be done by means of a copy of one of the documents set out in section 4.1.1.2 or by means of an authenticated signature.

When establishing a relationship with legal entities or legal arrangements, the Group must also take note of and document the contracting partner's power of attorney arrangements.

4.1.5. Identification and Verification of the Identity of the Beneficial Owner

4.1.5.1. Identification of Beneficial Owner

A beneficial owner is each natural person who is the ultimate, economic owner of the assets booked with or managed by the Group.

Subject to section 4.1.5.3, the Group shall inquire if there exists any beneficial owner in relation to a client.

For **natural persons**, the Group identifies all beneficial owners.

For clients that are **domiciliary companies**, the Group identifies all beneficial owners.

For clients that are operating **legal entities**, the Group identifies the beneficial owners as follows

(i) the natural persons (whether acting alone or together) who ultimately (directly or indirectly) own 25% or more of the legal person

(ii) to the extent that there is doubt under subparagraph (i) as to whether the natural persons who ultimately own the legal person are the beneficial owners or where no natural persons ultimately own the legal person, the natural persons (if any) who ultimately control the legal person or have ultimate effective control of the legal person

(iii) where no natural persons are identified under subparagraph (i) or (ii), the most senior member of the legal person's executive body must be identified.

For clients that are **legal arrangements**, the Group identifies the beneficial owners as follows

- for trusts, identify the settlors, the trustees, the protector (if any), the beneficiaries[14] (including every beneficiary that falls within a designated characteristic or class), and any natural person exercising ultimate ownership, ultimate control or ultimate effective control over the trust
- for other types of legal arrangements, identify persons in equivalent or similar positions, as those described in the subparagraph above.

In case of ownership layers, generally, the natural persons who own the last layer (domiciliary company, legal entity or legal arrangement) of the chain of ownership are identified as the beneficial owners.

4.1.5.2. Verification of Identity of the Beneficial Owner

The Group has to verify the identity of each beneficial owner.

If the beneficial owner is equal to the account holder, the verification of the identity has already been completed as described in section 4.1.1 and 4.1.2.

[14] In relation to a beneficiary of a trust, the Group shall obtain sufficient information about the beneficiary to satisfy itself that it will be able to establish the identity of the beneficiary
(a) before making a distribution to that beneficiary; or
(b) when that beneficiary intends to exercise vested rights.

Where the beneficial owner is not the same as the account holder, the identity of the beneficial owner must be verified as outlined in section 4.1.1 and 4.1.2. In such cases, the Group has to request a declaration in writing from the account holder declaring the identity of the beneficial owner. Whilst the Group relies on the account holder to declare the beneficial owner, the Group remains responsible to take reasonable measures to ascertain who the beneficial owner is, following the principles outlined in section 4.1.5.1 and using the relevant information or data obtained from reliable, independent sources (e.g. identification documents, shareholder register, official transparency register).

Each beneficial owner (current and/or former) must be recorded in the local beneficial owner database in a searchable way. The information as outlined in section 4.1.2 above has to be recorded.

4.1.5.3. Exceptions regarding the Identification & Verification of the Identity of the Beneficial Owner

The Group is not required to inquire if there exists any beneficial owner in relation to a client that is

- an entity listed on a Stock Exchange that is subject to regulatory disclosure requirements and to requirements relating to adequate transparency in respect of its beneficial owners (imposed through stock exchange rules, law or other enforceable means)
- a financial institution that is subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF
- a collective investment form and/or an investment vehicle with more than 20 investors and where the managers are financial institutions subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF.

unless the Group has doubts about the veracity of identification and verification information.

The rationale for the exception must be documented and retained.

4.1.6. Repeating the Identification and Verification Process

The Group has the duty to repeat the identification and verification of the account holder and/or the beneficial owner if doubts arise whether the information given concerning the identity of the account holder and/or beneficial owner is correct.

Unusual circumstances that can give cause for doubts include:

- The account holder grants a Power of Attorney (PoA) to a person who does not appear to have a sufficiently close relationship with the contracting partner. The granting of discretionary powers for asset management to a financial intermediary does not in general give cause for doubt,

- The Group knows the financial standing of the account holder and he deposits assets or expresses an intention to deposit assets that exceed the expected value.

If, in the course of a business relationship, the suspicion arises that the account holder has provided false information in relation to the ID&V of the account holder, beneficial owner or other parties as outlined in the sections 4.1.1 to 4.1.5, Compliance must be informed immediately.

4.2. Name Screening and Media Searches

Screening is a key stage of the CDD process, the outcome of which needs to be documented appropriately. It is a key determining factor whether a client poses a heightened risk such as being subject to financial crime related adverse media, possessing a high media profile or a political exposure etc. The media search may also support the KYC information with respect to the client's career path and business development etc. For further details regarding the principles, procedures and responsibilities of adverse media screening, reference is made to JBG-G-1026-03 Group Adverse Media Screening Guideline).

The screening and media search process (collectively referred to as "screening") is composed of the following elements:

- Name check (World Check and where available internal unwanted client lists as the underlying source of information)
- Business information and research tools such as LexisNexis or Factiva (where applicable)
- Open source search (Google, local open source search engines where applicable).

All natural and legal persons with KYC relevant roles have to be screened in line with the applicable guidelines. The KYC relevant roles subject to screening can be generally categorized into the following three groups:

- Account holders / Contracting parties
- Beneficial owners incl. controlling persons / settlors / founders / beneficiaries/ protectors etc.
- Power of Attorney / Authorized signatories.

The screening results must be documented either in an electronic or in a physical form. The rationale that led to the qualification of screening results (false positive vs. true match) and the categorization as well as risk assessment of the true matches have to be specified and comprehensible for any independent third party.

4.3. Purpose of the Client Relationship and Expected Account Activity

The Group needs to understand the overall purpose and the intended nature of the client relationship as well as the specific purpose of the account (e.g. wealth management, specific investment strategies, diversification of assets, mortgage). Information about expected account activities shall be provided, e.g. source and amount of initial account funding, types of transactions expected, and estimated frequency, average transaction amounts and jurisdiction of the transactions. In instances where the client has more than one account, the specific purpose and expected account activities for each account must be identified.

For clients that have no personal nexus or business relations to the country of the Group location where the assets are booked, a description of the rationale for opening an offshore bank account is required. Typical reasons include stability of the banking system or the currency, political stability, range of products and services offered, diversification of assets, recommendation by friends or service providers, etc. Where the RM is located in a Group location that is not a Booking Centre, the missing personal nexus is common and therefore generally requires less detailed description of the rationale.

It shall be further documented how the client was introduced to the Group, including the information whether an existing client of the Group, a finder (introducer), an EAM or an EFA was involved.

4.4. Client Background

The KYC profile must contain a consistent and coherent explanation of the personal and family background of the client. Their background (e.g. education, professional development and career) assists in understanding the wealth accumulation. The client's family background (marital status, children) is connected to the client's wealth and its future distribution and is also linked to potential wealth planning needs. Close associations (whether connected through family, personal, social or professional association) with any politically exposed persons shall be documented (reference is made to section 3.2.1.1).

4.5. Source of Wealth

The SoW is another key aspect relating to a client profile. SoW is the description of how the client's current wealth was generated over time. A comprehensive view on the client's SoW allows the Group to form a reasonable belief that the client has acquired his wealth from legitimate sources.

The story of the client's wealth accumulation needs to be consistent and detailed following a chronological order. The accumulation of main and any additional income streams during specific periods must comprehensibly lead to the client's overall wealth today. An integral part of the wealth accumulation story is the current breakdown of the assets of the client. The aim is to be able to substantiate the client's actual total wealth, broken down into asset classes. The numbers described in the asset breakdown must be plausible and correspond to the overall logic of the narrative.

It is important to note that the process of establishing SoW cannot be entirely standardized, and some degree of judgement has to be exercised, always considering the facts of each case and the unique profile of each client as well as the corresponding risk factors.

4.6. Source of Income

The Source of Income (SoI) of the client is a description of how the client's current annual income is generated. The Group is interested in the overall (global) income of the client, which is part of the ongoing generation of wealth. In cases where the client's income is (partially) transferred to the Group, it overlaps with the Source of Funds. Examples of SoI include salary, management bonuses, rental income, income from business activities, investment returns and others.

4.7. Source of Funds

The Source of Funds (SoF) refers to the origin of the funds deposited with the Group. The SoF also includes a description of the means of transfer of assets that are accepted into the account at the time of establishing a relationship, and the expected significant transfers during the course of the relationship.

4.8. Parties Connected to the Account

Details of parties involved in the client relationship and the relationship between such parties (e.g. power of attorney, signatory) and the client must be provided. The specific roles of such parties in a banking relationship must be clearly established. Further investigation needs to be conducted where such details raise questions about the ultimate beneficial ownership on the account, and if necessary, the case has to be escalated to local Compliance.

In particular, parties with Power of Attorney (PoA) may play an important role in a banking relationship and therefore may represent a risk factor. The following information shall be clarified:

- the relationship between the PoA and the client
- the reason for the appointment of the PoA
- whether the nature of the PoA relationship requires an EAM or EFA qualification

Where a PoA is granted to an immediate family member of the client (parent, spouse, children or siblings), typically a less detailed reason for the appointment is required. Nevertheless, such constellations may also raise questions about the ultimate beneficial ownership on the account, in particular where the client's SoW is derived from the PoA.

5. CORROBORATION

Corroboration measures involve obtaining independent verification information/documents supporting the legitimacy of the information provided by the client with regard to SoW. The narrative of the SoW in the KYC profile has to be convincing and the corroboration needs to support the main sources of the client`s wealth in line with the detailed provisions for the various client risk categories as listed below. Corroboration may be provided by the client, a third party or found in public sources. It may also include observations made by the RM himself/herself.

Following a risk-based approach, the level or strength of corroboration required depends on various risk factors, and in general, the higher the risk of the client the more robust the corroboration must be. It is important to note that the process of assessing and corroborating a KYC profile cannot be entirely standardized, and some degree of judgement has to be exercised, always considering the facts of each case and the unique profile of each client as well as the corresponding risk factors.

The narrative may be supported by primary and/or secondary corroboration (only primary or only secondary or a combination of both), depending on the specific case, but typically, solid corroboration consists of multiple sources.

Primary corroboration is the most reliable corroboration and includes documents issued by government bodies or public institutions, or by reputable, reliable professionals such as audit firms, lawyers, accountants or notaries when they act in their capacity of issuing or verifying official documents.

Secondary corroboration encompasses documents issued by any other sources (for further details on what qualifies as corroboration and the different types of corroboration refer to Appendix 5). Independent of the type of the corroboration provided, the sources must always be reliable.

Compliance may require additional corroboration based on its overall assessment of the underlying risks of the client relationship. Where it is not possible to collect the equired corroboration (specific requirements set out below in sections 5.1 to 5.3) for a specific client, the request to the client and explanation why this cannot be provided must be documented. The authority to accept or reject the client's explanation of missing corroboration lies with Compliance. There must be valid reasons for the unavailability of corroboration e.g. time passed, country specific record retention regulation. Where corroboration is required and the client is reluctant or unwilling to provide any corroboration, the RM shall escalate the case to his/her superior and Compliance.

5.1. For all Risk Clients

Corroboration (primary and/or secondary evidence) is required to support the storyline of the main accumulation of the client`s wealth. This means that a complete description of the SoW must be specified in the KYC (for details, reference is made to section 4.5.). Corroboration for the key stages of wealth accumulation of the client is required.

5.2. For PEP Clients

In addition to the above provisions for risk clients, the following guidelines apply for PEPs: Due to the underlying risks of the position of politically exposed persons, the Group must assess with greater care how the wealth of a PEP client has changed after the appointment to a public function. Relevant corroboration must also be requested for the wealth accumulation of the period after the appointment. The same logic applies for clients who are PEPs by association – an analysis must illustrate whether / how the wealth of the client has changed since the PEP took office and generally, if and how the client benefited from his connection with the PEP. For the definition of a PEP, reference is made to 3.2.1.1.

Where the client is a legal entity (or unincorporated structure), and such entity has close ties to a PEP, independent supporting documents are required to verify SoW. Such documents may include financial statements, annual reports, brochures, or other available information published by the company, articles from newspapers or magazines, or other reliable business information as detailed in Appendix 5.

5.3. For Standard Risk Clients

In case of gaps in the storyline in relation to SoW, the client must provide valid reasons for the unavailability of the information (inherited wealth that was generated decades ago, divorce settlements with limited information on how the wealth was generated etc.). In such cases, some level of corroboration is required for the available SoW elements.

Equally, where elements of the SoW description seem unusual, Compliance may require some level of corroboration.

6. REPORTING

6.1. General Reporting Duties

As part of the consolidated supervision, legal entities of the Group have to ensure a timely and appropriate reporting in the area of FCC. For further details regarding these group-wide reporting duties, reference is made to JBG-2000-00 Group Financial Crime Policy.

6.2. Reporting of PEP Relationships

The Group PEP Desk manages and maintains a database containing all known relationships associated with PEPs within the Group.

In addition, these relationships are reported once per year to the Chairman of the Group. Relationships associated with PEPs are reported by the legal entities on a quarterly basis to the Group PEP Desk. The Group PEP Desk discusses the list annually with the responsible Region Heads and reports the relationships with PEPs to the Group CRO for approval.

7. REVIEW OF EXISTING ACCOUNTS

7.1. Review Elements

When reviewing an existing account relationship as part of a periodic review, the following elements must be reviewed:

- KYC profile ("is it up-to-date?")
- Additional risk elements (if any)
- Results of name screening and media searches
- Account activities

The look-back period must cover the time since the last review respectively the opening of the account. If the client's actual use of the account is not consistent with the anticipated use identified at account opening or subsequent reviews, the RM must assess such deviation and, depending upon the outcome of the assessment, follow up with his/her superior and Compliance. In any case, the RM must update the KYC profile accordingly. The RM is required to escalate to his/her superior and Compliance, if they identify any concerns during the course of the periodic review, e.g. unusual transactions or unusual transaction patterns, or adverse results from name screening or media searches, non-alignment with the defined risk appetite e.g. Risk Tolerance Framework.

Certain Risk event may also trigger the review of an account relationship. The scope of the review triggered by a risk event may vary depending on the nature of the risk event itself.

For details, reference is made to section 7.2. Regarding the periodic review of Institutional Relationships, reference is made to the D-1152-00 Client Acceptance and Maintenance Policy for Institutional Relationships.

7.2. Periodic Reviews of Relationships

The reviews of a relationship follow a predefined process. Therefore, risk relationships have to fulfil higher requirements than relationships with standard risks, e.g. additional approvals within the review process. The following table outlines the required approvals to review a relationship:

PEP[15]	**Large Clients/ Sensitive Industry/ Commercial Accounts/ Complex Ownership Structure**	**Risk Country**	**Standard Risk**
Review cycle: **Annually** **Responsibility:** Performance and documentation of periodic review: • RM **Review & Approvals:** • Superior • Risk Country Market Head if risk country involved[16] • Local Compliance • Region Head[17] **Head Office** • Group PEP Desk • Group Chief Risk Officer (CRO)	**Review cycle:** **Every 3 years** **Responsibility:** Performance and documentation of periodic review: • RM **Review & Approvals:** • Superior • Risk Country Market Head if risk country involved[16] • Local Compliance • Region Head[17] [18]	**Review cycle:** **Every 3 years** **Responsibility:** Performance and documentation of periodic review: • RM **Review & Approvals:** • Superior • Risk Country Market Head[16] • Local Compliance	**Review cycle:** **Every 5 years** **Responsibility:** Performance and documentation of periodic review: • RM **Review & Approvals:** • Superior • Local Compliance

8. CLOSING OF RELATIONSHIPS

8.1. General Requirements

The closing of a relationship is not allowed if there are concerns or the suspicion of a connection to Financial Crime. In such cases, the RM must inform his/her superior and local Compliance upon receiving the closing request. Local Compliance reviews such concerns or suspicions and decides whether the account closing can be executed.

When transferring the assets in the course of a closing of a relationship, the Group ensures that there is a paper trail. Further, the reason of the closing shall be documented appropriately.

[15] The annual review of PEP relationships is initiated by the Group PEP Desk that coordinates the process in collaboration with local Compliance at the Booking Centres.
[16] If there are multiple risk countries involved, Risk Country Market Head approval for the identified key risk country is required (reference is made to section 3.2.4)
[17] Outside of Switzerland, where an account is managed by an RM who reports to a Region Head outside of the jurisdiction where the assets are booked, the approval of the Region Head responsible for the RM is sufficient.
[18] The Region Head may delegate his/her duty to review and approve the continuance of risk relationships; reference is made to the delegation principles in section 3.3.1.

8.2. Closing of Risk Relationships

Before closing relationships involving a PEP, the RM shall inform his/her superior and local Compliance. It shall contain details on who initiated the closing, the reasons for this decision and where the assets are transferred to. The RM ensures that this information is documented appropriately. Local Compliance assesses whether there are any obstacles that do not allow the closing of the relationship and informs the Group PEP Desk prior to the account closing. In case of a CUR set-up, Compliance at the Booking Centre, when closing the PEP relationship, must inform Compliance of the Advisory Location and the Account Manager in the Booking Centre accordingly. The same applies in cases where Compliance of an Advisory Location closes the PEP relationship.

For all other risk relationships, the RM shall review and document appropriately who initiated the closing and the reasons for the closing, where the assets are transferred to and whether there are any obstacles that do not allow the closing of the relationship. The RM must inform his/her superior and local Compliance in case of any concerns or suspicions in relation to the closing.

9. ACCOUNT MANAGEMENT GUIDELINES

All details related to opening, maintenance and closing of accounts such as required documentation and the specifics of the different account types are stipulated in local guidelines (to the extent applicable).

Appendices:

- JBG-2003-01 Sensitive Industries
- JBG-2003-02 List of Sanctioned and Risk Countries
- JBG-2003-03 Commercial Accounts
- JBG-2003-04 Summary of CDD and EDD measures
- JBG-2003-05 Corroboration Principles

FS JBG-2003 Private Banking Client Acceptance Policy