

COMPLIANCE

Conflict of Interests ("COI") Policy

Investec Bank (Mauritius) Limited

April 2024



DOCUMENT INFORMATION

Applicable to	DLC	n/a	Ltd	n/a	Plc	n/a
Document location	Shared Drive/Policy folder					
Version	3/2023					
Approved by	IBM Board					
Effective date	November 2023					
Review frequency	18 Months					
Owner(s)	IBM Compliance					
Author	IBM Compliance					
Superseded document	IBM Conflicts of Interest Policy – October 2022					
Notes	Applies to Investec Bank (Mauritius) Limited (IBM) and its subsidiaries					

Table of Contents

01	Introduction and purpose of policy	04
02	Organisational scope/application	04
03	Definitions	04
04	Policy contents	
	4.1 What is a COI?	04
	4.2 Identification of COI	05
	4.3 Management of COI	05
	4.4 Conflict of interest – Directors	06
	4.5 Related Documentation	07
	4.6 Breaches and non-compliance	07
	4.7 Policy Updates	07

Conflict of Interests (COI) Policy

1. Introduction and purpose of policy

As an international, specialist banking and investment management group that provides a diverse range of financial products and services to a select client base, Conflict of Interests ("COI") are inherent to the Investec business. This inherence of COI is apparent given the nature of Investec's business, and that it simultaneously conducts the activities of proprietary trading, investment management, lending and

As a financial institution and good corporate citizen Investec Bank (Mauritius) Limited ("IBM") has both regulatory and fiduciary obligations to ensure that all potential or actual COI to which it is party are identified timeously, mitigated where possible, and appropriately managed.

The COI Policy has been implemented to adequately manage and mitigate COI. Failure to comply with the policy could result in regulatory, technical or procedural breaches, same may be regarded as unethical and cause reputational risk for Investec.

Certain Business Units (BUs) may apply stricter policies/procedures than is contained in the Investec Group Conflict Policy. It is the employee's duty to familiarise themselves with those policies/procedures applicable to them.

Given different regulatory requirements, Investec Bank Mauritius Limited ("IBML") has their own policies which aligns with the Investec Group's policies in all material aspects.

These are to be reviewed and approved by the IBML Board as well as the Compliance Policy Review Committee ("CPRC").

2. Organisational scope/application

This Policy applies to all IBM Employees and directors, including employees of any subsidiary.

3. Definitions

Please refer to Schedule 6 of the Group Market Conduct Policies for Abbreviations and Definitions.

4. Policy contents

4.1 What is a COI?

A "COI" describes a situation where two or more interests are legitimately present and competing or conflicting. This undermines the principle that all players in the market should have equal opportunity and status.

In financial institutions COI typically fall into one of the following 4 categories or a combination of these categories:

- **Firm (IBM) versus Client:** This form of conflict may arise where trading businesses act on both a principal and

agency basis and traders may have an interest in putting the firm's interests ahead of the clients when working a client order.

- **Client versus Client:** This can occur where two IBM clients are on opposing sides of a transaction and IBM wishes to advise both parties (for example, where one IBM client wishes to buy another IBM client) or where IBM is approached by two different clients to advise and/or finance the acquisition of the same target company. It may be possible to manage the conflict through Chinese Walls or by creating a 'Chinese Box' within each advisory team, however it is also possible that one team could be required to stand down due to the perception risk surrounding the conflict (i.e., the perception that information may be shared between the two teams) or due to regulatory requirements.
- **Employee versus client:** This type of conflict usually occurs due to an employee's shareholding or directorship of a company (for example, where an advisory client is looking at a transaction where an IBM employee is a director/major shareholder of the counterparty). Such conflicts are mitigated through the PA Dealing Policy and Outside Business Interests Policy. Otherwise, the resolution of such conflicts is usually treated on a case-by-case basis.
- **Employee versus Firm (IBM):** This type of conflict usually occurs in circumstances similar to those detailed above relating to Employee versus Client conflicts but may also arise in respect of the misuse of proprietary information of the firm. The former type of conflict is mitigated through the PA Dealing Policy and Outside Business Interests Policy. Otherwise, the resolution of such conflicts is usually treated on a case-by-case basis. The misuse of proprietary information is dealt with elsewhere (for example in the Investec Dlc Information and Technology Policy).
- **Employee versus Employee:** This type of conflict may occur where there are Personal Relationships (which is defined as any intimate, romantic or sexual relationship which goes beyond the normally accepted boundaries of relationships between friends, colleagues, and close family relationships) or Familial Relationships (defined as a spouse, domestic partner, parent, child, sibling, grandparent, grandchild, in-laws, and stepparent, step child, guardian and ward, or member of one's household; extended family, such as cousins, aunts and uncles; having a close friendship or relationship with someone) between colleagues. For example, this would include employees who supervise, lead, manage or have direct influence on the decision making for another employee with whom they are in a personal relationship (including but not limited to hiring, performance management or reward). The purpose is to ensure that any potential conflicts arising from personal or familial relationships at work are identified and can then be appropriately managed. This includes managing situations that have the potential to lead to COI, discrimination or claims of harassment and/or compromising segregation

of duties. This type of potential conflict is mitigated through the personal relationship disclosure to Senior Management or Human Resources (HR).

Where a financial institution has a COI between itself and its client, or between one client and another client, the financial institution must act with due regard to the interests of each client and manage the COI fairly. Investec employees are required to act in the best interests of Investec and its clients at all times.

4.2 Identification of COI

To adequately manage COI, IBM must identify all relevant COI timeously. The primary responsibility for the identification of COI lies with the business, and in particular senior management for employees. IBM COSec is responsible for identification and recording of director's COI.

Investec employs different mechanisms to ensure that all COI are identified, inter alia:

- IBM Compliance maintains a Matrix Index of potential COI risks i.e., COI Risk Management Plan at Investec, taking into consideration all BUs and income streams. The index is a matrix of COI classified by COI type and business area with documented controls. The index is updated with all new COI identified and is reviewed on an annual basis.
- All employees, including compliance officers and management, are responsible for identifying specific instances of COI and are required to notify their IBM Compliance of any COI they become aware of. IBM Compliance will escalate the COI to Group Compliance to assess the implications of the COI and how the COI should be managed.
- COI Clearance Process – As with all COI, the primary responsibility for the identification of COI lies with IBM. To assist in this process, Group Compliance has established a COI Clearance process which requires a conflicts check to be completed prior to Investec signing a Non-Disclosure Agreement (“NDA”) with a client in respect of any potential transactions. If the transaction details are only made available to the deal team after the NDA has been signed, a conflicts check must be completed ahead of signing a mandate with the client.
- Various fora are in place at Group and IBM to interrogate any conflicts that may arise at the inception of new products to be distributed, such as: Group Deal Forum and IBM Credit Committee.
- Disclosure of Personal and Familial Relationships at work applies to all employees, directors, consultants, contractors, freelancers, interns and agency workers of Investec, regardless of seniority. To make such a declaration, staff are asked to inform Executive Management or HR. This can be done verbally or in writing. The leader and HR would work with the individual to determine any other parties that need to be informed. Staff who are uncertain about whether they need to declare a personal relationship or have other questions may discuss the matter in confidence with Executive Management or HR. The process is further articulated and aligned to Becoming Acquainted with Investec Mauritius (“BAWI Mauritius”) document.

In determining whether there is a COI, IBM Compliance and Senior Management will consider the factual circumstances and determine whether Investec or the affected employee:

- is likely to make a financial gain, or avoid a financial loss, at the expense of a client;
- has an interest in the outcome of a service provided to a client, or a transaction carried out on behalf of a client, which is distinct from the client's interest in that outcome;
- has a financial or other incentive to favour the interest of the firm, or a client or a group of clients over the interests of another client;
- carries on the same business as a client; and
- receives (or will receive) from a person other than a client an inducement in relation to a service provided to the client other than the standard commission or fee for that service.

4.3 Management of COI

Once a COI has been identified it must be appropriately and adequately managed.

IBM Compliance assesses each COI, including whether the COI is actual or perceived as well as the potential reputational risk. IBM Compliance and management then agree on the controls that need to be put in place to manage the COI, including the introduction of information barriers, recusals, implementation of policies/procedures, training and the like.

Specific instances of COI may require management intervention in addition to the documented controls already in place. These can include escalation to a management forum, such as the Executive Risk Committee (“ERC”) and/or other relevant forums, such as Investment Committee and Group Credit, for a decision on how the COI should be managed.

There is no single approach to dealing with COI. Each case is dealt with according to the nature of the COI and the perceived and/or potential risk. When a COI arises in the course of a transaction or business dealing, the following general principles are applied:

- Employees will have access to, and are entrusted with, confidential information in respect of both IBM and its clients. This information includes IBM and client dealings, transactions and trade secrets, and although the information may not qualify as “price sensitive” it remains confidential information. Employees cannot divulge this information outside of the normal course of their employment, and that the information cannot be used for either personal, familial or related party gain;
- Employees must be discreet with information, specifically price sensitive information, and not discuss it in public places where it can be overheard such as elevators, restaurants, taxis, airplanes and the like. Information should be treated as confidential even in the normal course of employment;
- Financial services should be provided in a manner that will not advance the interests of one client unfairly over the interests of another client;
- Clients should be treated fairly, and IBM should manage COI between the interests of various clients (including existing or potential clients);

- COI should be managed in the best interests of clients, above all else;
- Client interests are always prioritised ahead of Investec interests, which in turn are always prioritised ahead of employee interests; and
- IBM should ensure that clients are appropriately informed about any COI that may affect the provision of financial services to them.
- Disclosure of Personal and Familial Relationships at work, which is part of the on-boarding process for all new joiners to be followed by all employees.
- a clean desk policy is strictly adhered to where Chinese boxes have been established; and
- any reporting of work in progress, committee papers, etc., should be restricted in content and audience as regards sensitive information pertaining to the affected deals.

The best means of managing a COI will depend on the nature of the COI in question and the parties involved. Steps that can be taken to manage COI include, but are not limited to:

- **No COI exists/touchpoint:** On occasion, after further investigation, it may be concluded that an apparent COI does not exist or it may be deemed to be a touchpoint rather than a COI (i.e., two business areas may have a relationship with a company, however these relationships may not necessarily conflict with each other to create a COI).
- **Disclosure of the COI and/or how it is managed:** Although disclosure serves to mitigate the COI it is neither the only nor the most effective method of doing so. Disclosure of the COI should be made if it will minimise the impact of a COI, such as:
 - disclosure can be made directly to the affected party or within a public document;
 - disclosure must be adequate, clear, and concise to enable the recipient to fully understand its relevance; and/or
 - disclosure should be timeous (i.e., occur before/when the service is provided).

Evidence of the verbal and/or written disclosure to the affected party must be submitted to IBM Compliance for recordkeeping.

Note: Employees must seek advice and guidance from IBM Compliance and/ or IBM Legal prior to disclosing an existing or potential COI.

- **Informed consent:** Where a client could be affected by a COI (either actual or perceived), it may be possible to proceed with the proposed transaction subject to the client's consent (after full disclosure of the COI with the guidance of IBM Compliance).
- **Deal trees:** For certain COI that may occur within IBM, it may be possible to manage them by enforcing information barriers in the form of deal trees. In effect, this segregates different deal teams within IBM through the establishment of information barriers.

Deal trees may not be suitable for all engagements. IBM Compliance should be consulted to implement such controls. In practice, this would generally involve, inter alia:

- electronic segregation of the deal teams – deal teams would need to set up restricted folders which allow access only to members of the deal team;
- discussions should be held away from the rest of the team in secure meeting rooms;
- sensitive phone calls should not be made from the desk where there is a risk of being overheard;

- **Stand down:** Occasionally it will either not be possible to resolve a COI satisfactorily or the perception of a COI will be too great to enable a transaction to proceed. In these circumstances it will be necessary for one of the conflicting areas to stand down from the transaction.
- In circumstances where the employee's OBI/EP or any other relationships with a party linked to a proposed transaction is regarded as an actual/perceived COI, the COI must be declared to IBM Compliance, BU Head as well as the Chief Operating Officer (COO) in material instances for management of the perceived/actual COI. Management of the COI will require disclosure to or recusal from credit and/or other forums where the pending transaction/ contract negotiations are discussed.

IBM Compliance maintains records of all COI identified and their resolution, including the persons involved and the controls used. This information is included in reports to Senior Management.

4.4 Conflict of interest – Directors

Directors (including non-executive directors of IBM) must, as far as possible, avoid conflicts and where a conflict or potential conflict arises, the same must be disclosed and all procedures for dealing with such cases must be strictly adhered to. Directors who are conflicted regarding a particular issue should not participate in the related discussions and decision-making.

A conflict of interest may occur when:

- A director's personal interest is adverse to or may seem to be adverse to the interests of the Company.
- A director, or a member of his or her immediate family, receives improper personal benefits as a result of his/her position in the Company.

Some of the common conflicts directors should avoid are listed below:

- Personal benefits received from a person/ Company seeking to do business or to retain the services of the Company.
- Gifts which are not customary in normal business relationships should not be accepted nor given to any person/Company seeking to do business or to retain the services of the Company.
- Engaging in any outside business, professional or other activities that would directly or indirectly adversely affect the Company.

Personal financial interests should be declared to the Company Secretary and any material changes should be proactively reported to the Company Secretary. The Company Secretary coordinates and maintain records of declaration of directors' interests.

4.5 Related Documentation

The following policies are the controls adopted by Investec to manage and mitigate COI:

- Becoming Acquainted with Investec Mauritius (“BAWI Mauritius”).
- IBM Personal Account (“PA”) Dealing Policy
- IBM Gifts & Entertainment Policy
- IBM Outside Business Interests (OBI) Policy
- PLC and INL (“Investec Group”) Policy on Conflicts of Interest.

Employees should refer to applicable IBM policies and procedures for further information.

4.6 Breaches and non-compliance

Non-compliance with the COI Policy is regarded as a breach. Both the employee and the employee’s line manager will be notified of any instances and any repeat offences can result in disciplinary action against the employee.

Employees must report any actual or suspected breach of this Policy, committed by themselves or another employee to IBM Compliance.

4.7 Policy Updates

This policy is reviewed and approved on an 18 months basis. Changes may be recommended at any time as and in response to changing circumstances. The policy is approved by the IBM Board and tabled for noting at the Compliance Policy Review Committee whenever there are material changes to the policy.

