2026

Contents

1. THE GROUP

KBC Group is an integrated banking and insurance group, catering mainly for retail, SME and midcap customers. It concentrates on serving its home markets: Belgium, Czechia, Slovakia, Hungary and Bulgaria. Elsewhere around the globe, the group has established a presence in selected countries and regions. KBC Group is regulated by both the National Bank of Belgium (NBB) and the Belgian Financial Services and Markets Authority (FSMA); it also falls under the supervision of the European Central Bank (ECB).

2. INTRODUCTION

The cornerstones of the KBC Group strategy are based around building trust, promoting and embedding responsible behaviour in every aspect of its operations. In today's digital world, financial organisations like KBC Group are prime targets for fraudulent attacks due to the significant assets and sensitive data they manage. Recognising this, we place the integrity of our operations and the protection and interests of our stakeholders and our customers, at the forefront of our fraud risk assessments and policy implementations. Fraud Risk is an integral part of KBC's Risk Management Framework and has been designed and implemented to provide comprehensive protection for the group's assets, as well as those of its employees, customers, suppliers and stakeholders. That is vital in a rapidly changing environment where digitalisation has created new attack vectors and an increase in threats targeting both the organisation and its customers.

3. DEFINITIONS

Fraud risk[1] is the risk of deliberate abuse of procedures, systems, assets, products and/or services by one or more persons who intend to deceitfully or unlawfully obtain an advantage, avoid an obligation or cause financial or non-financial damage. This can apply to:

- **Internal Unauthorized activity**: Internals intentionally/deliberately exceeding/abusing authority when entering, approving or not reporting a transaction, rogue trading and intentional mismarking (in securities valuation).
- **Internal Theft:** Theft (of money, property or time) attempted or perpetrated against the organization by internals, including instances where an internal is acting in collusion with external parties.
- **External Fraud**: Fraud attempted or perpetrated by an external party (i.e. a party without a direct relationship to the financial institution) or by a customer of KBC without the involvement of an employee or affiliate of the organization, in which the financial institution, its products, or its processes are misused to facilitate fraudulent activities, regardless of whether the financial harm is suffered by the institution, its customers, or an external party.

[1] In this context, fraud risk is excluding tax fraud and information security/IT risk which are governed by their dedicated frameworks.

4. FRAUD RISK MANAGEMENT

4.1. Fraud Risk Management process in KBC

By nature, fraud risks are present throughout the whole organization in every entity, domain, process and activity – as they are an integral part of 'being in business' and 'running the organisation'.
By managing these fraud risks and by safeguarding our operational resilience, KBC can provide a continuous service and hence protect KBC, its clients and counterparts from losses, disruptions, etc... By doing so, we also contribute to the overall stability of the financial sector in regions we are active.

Fraud risk is managed under KBC's Operational Risk Management Framework ('ORMF'), with a dedicated Operational Risk Standard on Fraud Risk Management. Anti-Money Laundering, Know Your Customer (KYC), Know Your Transaction (KYT) and ethics remain governed by compliance policies (in line with regulation).

Both need to be read in conjunction and set the standard for building and maintaining a strong control environment throughout the KBC Group. It defines among others the required governance, organization and core risk management processes. Its aim is to ensure that KBC takes all necessary steps to protect the good name, reputation and assets of KBC group entities and those of its employees, customers, suppliers and other stakeholders. This methodology also ensures a uniform, consistent and transparent approach across all KBC entities.

Managing fraud risk is a continuous process with several steps, being (1) risk identification, (2) risk measurement, (3) setting & cascading risk appetite and (4) risk analysis, reporting, and follow-up.

4.2. The identification of fraud risk

This relates to the timely identification of risks that can harm a legal entity or customer of KBC Group. There are numerous sources that are used to structurally capture fraud risks within KBC Group. When potential fraud risks are identified, business should respond to these events depending on their impact and likelihood, e.g. by strengthening controls – as also described in the next parts of this document.

Special attention needs to be given to collecting and sharing fraud threat intelligence. Understanding the modus operandi of fraud schemes helps in identifying, preventing and mitigating fraud risks by recognizing recurring tactics and vulnerabilities exploited by fraudsters. To stay ahead of the new modus operandi, it is important that for both the internal and external cases, the necessary analyses are performed and shared within the KBC community.

4.3. Risk measurement

Risk measurement entails an assessment which risks are more critical than others (based on potential impact and likelihood), and for which controls must be in place. Once a fraud risk is identified, the accountable manager needs to assess the risk, and see if there are controls in place to manage the risks. A view on all outstanding risks shows then what the current overall risk exposure is (i.e. the risk profile). This risk profile should be within the defined risk appetite (see next bullet).

Next to the current fraud risk profile, it's essential to complement this also with a forward-looking aspect. This proactive approach should give an estimate of the potential exposure of KBC to (future) fraud risks if no additional risk responses are considered.

4.4. The setting and cascading of the risk appetite

Once the risks are identified and assessed, we need to evaluate whether these risks are within our risk appetite. For operational risk this is done by aggregating the residual risks towards the risk profile and by installing uniform indicators that are measured and monitored. This risk appetite is decided by the KBC Group Board of Directors for KBC Group, KBC Bank and KBC Insurance. At local level, the risk appetite is approved by the local supervisory board[2].

4.5. Risk analysis and response, reporting and follow-up

Identified risks will need a response from business on how they will manage the risk, meaning how KBC will manage/react to the actual residual risk as compared to its risk appetite. For concrete fraud cases, management needs to ensure as well that there is a consistent and systematic approach to handling fraud cases, providing clear guidance on actions to take when fraud is suspected or detected. This also entails having a clear fraud governance. Effective fraud prevention involves a well-structured organization with clearly defined areas of authority and proper reporting lines. Sufficient attention and focus on fraud should be ensured and fraud awareness and fraud education should be foreseen on a regular basis.

[2] If the local supervisor has defined a different committee for this role, this committee takes precedence.

Risk evolutions are constantly monitored to be sure that our view on fraud risks evolves in sync with the world around us.

The result of risk responses and risk evolutions are regularly reported and followed up in committees made up of senior management, including the chief Compliance Officer, the Chief Risk Officer, and top executives of the business units responsible for managing the operational processes. On top of this, also quantitative fraud reporting is in place where specific key indicators on fraud risk are reported consistently, timely and comprehensive, enabling effective oversight and informed decision-making. Reporting and follow-up is crucial to ensure the control environment remains strong in a changing internal/external environment, so that the residual risks remain within the operational risk appetite.

Fraud cases are assessed case-by-case and reported to competent authorities in line with applicable laws, regulatory obligations and internal procedures.