Summary of

Reputational Risk Policy

1. Objective and Scope

This summary of the Reputational Risk Policy serves as a brief summarization of the detailed internal Reputational Risk Policy of the Hamburg Commercial Bank AG for external reference.

The Reputational Risk Policy aims to identify, assess, manage and mitigate or prevent actual or potential impacts arising from reputational risks inside Hamburg Commercial Bank (hereafter "the Bank"). The policy applies to all employees that are part of the Hamburg Commercial Bank Group (meaning all its subsidiaries and foreign locations/ branches). Overall, the policy is embedded in and complemented by HCOB's Code of Conduct, Related Party Transactions Policy and Conflicts of Interest Policy.

Reputational risks are the risks arising from the negative perception on the part of a relevant stakeholder group that can adversely affect the Bank in the form of reduced profit or a loss or reduction of deposits. Reputational risks can arise within the entire Bank and should therefore always be considered.

The relevant stakeholder groups are the customers, creditors, supervisory authorities, owners and staff of the Bank, as well as the public, rating agencies and representatives of the media.

Through their actions, all employees are responsible for building and maintaining a good bank reputation.

2. Tasks, competences and responsibilities

The different tasks such as conducting reputational risk analyses and performing proper documentation are to be performed by all employees. Particular responsibility falls within the business unit Risk Control with the respective Non-Financial-Risk (NFR) Circle to be involved in decisions regarding critical cases. Permanent voting members of the NFR Circle are the Head of Risk Control as well as the Chief Risk Officer.

3. Identification and analysis of reputational risk

The reputational risks analyses are primarily based on inquiries, press reports, publications of the customer or business partner or the sector, certifications and international standards or conventions or other appropriate documentation.

With the establishment of overall guidelines, the persons dealing with the identification of reputational risks are supported, so that they can distinguish within a consistent framework between unproblematic, problematic, unwanted and banned business cases.

3.1 Overall Guidelines

In addition to existing regulations, the criteria listed below provide binding standards for the assessment of transactions and business partners of the bank.

These are based on

- the ten principles (P01 to P10) of the United Nations Global Compact
- exclusion criteria (e.g. HCOB's blacklists for countries and industries)
- further internal checklist

3.1.1 United Nations Global Compact

The bank observes the 10 principles of the Global Compact as follows:

The bank supports and respects the protection of international human rights (P01) and ensures that its activities do not result in breaches of human rights (P02). In line with this, the bank will also have no business relationships with business partners that breach human rights.

Furthermore the bank upholds freedom of association and recognition of the right to collective bargaining (P03) and promotes an end to forced labour (P04), child labour (P05) and discrimination in employment and occupation (P06). Consequently, the bank will have no business relationships with business partners who breach the principles P03 to P06 or make use of illegal employment practices (undeclared labour) and therefor go against the International Labour Organization's Declaration on Fundamental Principles and Rights at Work.

The bank takes a precautionary approach to environmental challenges (P07), undertakes initiatives to promote greater environmental responsibility (P08) and encourages the development and diffusion of environmentally friendly technologies (P09). The economic, ecological and social performance of a society can only be ensured, if scientific, environmental and social objectives are pursued across generations at the same time and given equal weight. In keeping with this, the bank will have no business relationships with business partners that, for example, breach local environmental laws, manufacture banned products such as CFCs or asbestos or have projects that encourage illegal tree felling/ illegal slash-and-burn farming. This relates both to the primary cultivation, mining and production process as well as - insofar as the bank can detect it - the trade and further processing of such raw materials and goods. Against the background of the decision in 2011 by the Federal Government to withdraw from nuclear energy, the bank will also not participate in the financing of construction, extension or modernisation of nuclear power plants.

Lastly, the bank opposes every form of fraud, bribery and corruption, as already explicitly stated in the Code of Conduct (P10). Thus, it also does not participate in businesses for which there is a suspicion that these are associated with bribery. The requirements in the Anti-Fraud policy and Benefits policy must also be observed.

Additional exclusion criteria are listed in the Bank's Blacklist which can be found in the most recent ESG Factbook on the website and is anchored in the lending process. In context of the Blacklist the Bank also avoids business relationships that are tied to criminal or illegal activities such as illegal gambling or pornography. Furthermore, banned weapons and ammunition is excluded as well as speculation in agriculture raw materials and food markets. Lastly, the Bank ensures that the requirements of tax legislation are complied with.

3.1.2 Identification of transactions and projects with reputational risks

A template for the identification of the aforementioned reputational risks can be used to test whether aspects damaging to the Bank's reputation are present.

3.1.3 Impact analysis and assessment of reputational risk

Since the bank operates as a company in the field of tension between business interests and the ethical expectations of their stakeholder groups, reputational risks cannot be entirely avoided. At the same time, they cannot be directly managed by a quantitative limit. The objective of management of reputational risks is in principle to exclude them as far as possible or to reduce them.

Beyond that, the goal is to identify potential issues that might damage reputation, in order to react to them appropriately and thereby keep negative effects on the reputation of the bank as low as possible. For these purposes, primarily existing instruments are used, such as the risk event database, central complaints management and the whistleblowing system. RepRisk Controlling undertakes the monitoring of implementation of agreed measures for risk reduction.

The central reporting of reputational risks to the NFR Circle is carried out quarterly, based on different indicators and the quarterly all business unit managers query. In addition, major processes are reported in the Management Reporting Package. The quarterly reporting Non-Financial Risks informs on reputational risks.

From an overall perspective, the CRO is responsible for managing reputational risk. However, the operative handling of reputational risks is decentralized in the bank, since in principle every business unit and every subsidiary is responsible as “1st line of defense” for its business operations and associated risks. Correspondingly, the departmental managers are responsible for the development of maintenance of the good reputation of the bank in their area of responsibility. Simultaneously all employees need to contribute to reduce reputational risk by forward-looking behavior.

In the annual review of commitments, the business unit Risk Control checks adherence to the reputational risk guideline. In principle, not every RepRisk analysis needs to be documented. In cases of doubt, the analysis should be documented. In the event of reputational damage, documentation is required.

Hamburg, December 2023