Description of the Internal Control System in mBank S.A.

The internal control system is one of the elements of the Bank's management system. It helps the organisation to ensure effective and efficient execution of business processes. It covers all organisational units and sets out rules governing cooperation between them as well as the flow of information and monitoring of activities taking place in the Bank.

The principles and objectives of the internal control system arise from:

- the Banking Law Act, Regulation of Finance,
- Funds and Regional Policy of 8 June 2021 on the Risk Management System, Internal Control System and Remuneration Policy in banks, and
- Recommendation H of the Polish Financial Supervision Authority concerning internal control systems in banks.

The internal control system ensures:

1) efficient and effective operation of the Bank,
2) reliable financial reporting,
3) compliance with the Bank's risk management rules,
4) compliance of the Bank's operations with the law, internal regulations and market standards.

I. Roles of the Bank's authorities

1) The Supervisory Board:

   a) exercises supervision of the implementation and operation of an adequate and effective internal control system in the Bank,
   b) approves the rules of evaluation of the adequacy and effectiveness of the internal control system,
   c) performs an annual evaluation of the adequacy and effectiveness of the internal control system,
   d) approves the rules of classification of irregularities identified by the internal control system,
   e) approves proposals of the Management Board of the Bank concerning the fundamental organisational structure of the Bank,
   f) evaluates the degree of effectiveness of compliance risk management in the Bank,
   g) approves the mBank S.A. Compliance Policy, the mBank S.A. Compliance Department Rules and the mBank S.A. Audit Charter.

2) The Audit Committee of the Supervisory Board:

   a) monitors the adequacy and effectiveness of the internal control system based on

information and reports provided in particular by:
- the statutory auditor,
- Non-financial Risk Management Department,
- Compliance Department and
- Internal Audit Department,

b) issues opinions on the adequacy and effectiveness of the internal control system for the purposes of the evaluation of the system by the Supervisory Board.

3) The Management Board:

a) designs, implements and ensures in all organisational units of the Bank an adequate and effective internal control system within three lines of defence,
b) ensures the operation of a uniform internal control system in the Bank and the subsidiaries,
c) ensures continuity of the internal control system including adequate cooperation of all employees of the Bank within the control function and cooperation with the Compliance Department and Internal Audit Department, and ensures that employees of those units have access to necessary source documents, including documents containing information protected by law in connection with the performance of their professional duties,
d) defines the rules of evaluation of the adequacy and effectiveness of the internal control system,
e) defines the types of measures taken to eliminate irregularities identified by the internal control system, including corrective and disciplinary measures,
f) reports to the Supervisory Board, at least on an annual basis, on the performance of the tasks referred to in (a) – (e),
g) approves the criteria of identification of significant processes and the list of significant processes identified by the Bank and their links to the general objectives and the specific goals of the internal control system. Ensures regular reviews of all processes running in the Bank to check their significance,
h) approves the rules of classification of irregularities identified by the internal control system,
i) defines the rules of designing, approving and implementing control mechanisms in all processes running in the Bank, including definitions of the roles of organisational units responsible for designing, approving and implementing control mechanisms and for ensuring the adequacy and effectiveness of control mechanisms in processes running in the Bank,
j) defines the rules of independent monitoring of the observance of control mechanisms, including ongoing verification and testing,
k) ensures the functioning of a control function matrix in the Bank,
l) defines the rules of reporting on the effectiveness of the key control mechanisms and the results of their vertical testing,
m) takes responsibility for effective management of compliance risk,
n) approves and ensures compliance with the mBank S.A. Compliance Policy, the mBank S.A. Compliance Department Rules and the mBank S.A. Audit Charter,
o) ensures the independent position of the Compliance Department and the Internal Audit Department in the organisation of the Bank, defines formal authority and responsibilities of employees of the Compliance Department and the Internal Audit Department and the independence and appropriate status of the Director of the

Compliance Department, the Director of the Internal Audit Department and their employees.

II. Setup of the internal control system

The Bank's internal control system is based on three independent lines of defence, where:

1) the first line of defence is comprised of risk management in the operations of the Bank performed by the Bank's business units and units supporting them directly,
2) the second line of defence is comprised of at least risk management by designated organisational units or designated employees of organisational units, which takes place independently of the risk management in the first line of defence and operation of the compliance unit, i.e. the Compliance Department,
3) the third line of defence is comprised of the Internal Audit Department which is responsible for an independent evaluation of the adequacy and effectiveness of the risk management system and the internal control system in the first and second line of defence.

In all three lines of defence, the Bank's employees apply control mechanisms or monitor the observance of control mechanisms independently in pursuance of their professional duties.

III. Control function

The control function is a part of the internal control system. It comprises of all control mechanisms in processes running in the Bank, independent monitoring of the observance of such control mechanisms and the relevant reporting. It is performed in particular by positions, groups of employees and organisational units responsible for tasks assigned to the function.

IV. Scope of responsibilities and independence of the Compliance Department and the Internal Audit Department

a\ Compliance Department

Compliance is one of the objectives of the internal control system; it is understood in the Bank as ensuring compliance with the law, internal regulations and market standards by means of the control function and management of compliance risk, respectively.

Compliance by means of the control function is ensured by each employee of the Bank in the three lines of defence in compliance with applicable laws, internal regulations and market standards by designing, applying and modifying control mechanisms and independent monitoring of the observance of control mechanisms in line with the assigned responsibilities.

Tasks of the Compliance Department:

1) developing and implementing guidelines, including the policy, rules and standards of operation in the compliance area, and aligning them with the requirements of Commerzbank AG Group, subject to local legal requirements,
2) taking action in response to identified breaches of the policy,
3) advising bank units in its area of responsibility,
4) performing the control function by applying:

- DC's control mechanisms,
- independent monitoring of control mechanisms of the first and second lines of defence,
- documenting and reporting inspection and test results, and
- identifying and reporting irregularities, in particular material and critical ones,

5) carrying out compliance training, in particular training required by regulators or under the standards of Commerzbank AG Group, and monitoring the training completion by the bank employees,
6) issuing opinions on internal regulations, in particular rules and templates of agreements on products offered by the bank, in terms of their compliance with the law, supervisory requirements and market standards,
7) maintaining contacts with external supervision authorities (among others, the Polish Financial Supervision Authority (KNF)) in the scope arising from the law and the scope of DC's responsibility,
8) coordinating or conducting internal investigations concerning reported employee violations and employee fraud,
9) cooperating with the compliance unit of the parent entity, among others, coordinating tasks arising from standards of Commerzbank AG Group in the compliance area,
10) supervising compliance units in mBank Group subsidiaries in the scope of implementing common compliance standards in mBank Group within the DC's scope of responsibility, and personal data protection, in cooperation with the Personal Data Officer,
11) cooperating with other units of the bank playing a key role in the compliance assurance process.

b\ Internal Audit Department

Internal audit in the Bank is understood as independent, objective assurance and advisory actions taken in order to create value and improve the operations of the Bank.

Internal audit supports the Bank in the pursuit of its goals by means of a systematic and disciplined approach to the audit, assessment and improvement of the effectiveness of risk management, internal control and corporate governance processes.

Tasks of the Internal Audit Department:

1) assessing the adequacy and effectiveness of the risk management system,
2) assessing the adequacy and effectiveness of the internal control system,
3) performing scheduled and ad hoc audit tasks with respect to a particular audited area or particular audited areas,
4) making post-audit recommendations, monitoring and reporting on their implementation,
5) advising in the scope of the risk management system and the internal control system,
6) reporting on the results of inspections and status of implementation of recommendations made after certain inspections of the Polish Financial Supervision Authority (KNF) and statutory auditors,
7) cooperating with the internal audit units of the parent entity and subsidiaries in the scope arising from the Department's competence, the necessity to meet requirements defined in the regulations concerning consolidated supervision, and the need to carry out joint audits in order to provide expert support within the audits conducted,

8) coordinating works connected with inspections conducted by external control authorities.

c/ Independence of the Compliance Department and the Internal Audit Department

Independence of the Compliance Department and the Internal Audit Department is ensured by, among others:

1) reporting to the Bank's Management Board, Audit Committee and Supervisory Board,
2) possibility of direct communication between the Director of the Internal Audit Department and the Director of the Compliance Department and the Members of the Bank's Management Board, Audit Committee and Supervisory Board,
3) participation of the Directors of both departments in meetings of the Bank's Management Board and the Audit Committee, whenever such meetings concern issues related to the internal control system, including compliance, internal audit and/or risk management,
4) requirement that the appointment of the Director of the Internal Audit Department and the Compliance Department should be approved by the Supervisory Board and that their dismissal should be preceded by a hearing of those persons by the Supervisory Board,
5) separation of the Internal Audit Department and the Compliance Department from other organisational units, functions and positions in the Bank and a ban on performing obligations other than those resulting from their scope of responsibilities imposed on the employees of those departments,
6) approval by the Management Board and the Supervisory Board of the Bank of the Audit Charter specifying the operational rules of internal audit in mBank S.A. and the mBank S.A. Compliance Department Rules,
7) rules on hiring employees in both departments, which ensure independent and objective performance of tasks and an appropriate level of competence, experience and skills.

V. Rules governing the annual evaluation of the adequacy and effectiveness of the internal control system

The evaluation of the adequacy and effectiveness of the internal control system in the Bank includes an evaluation of the effectiveness of the control function, the compliance function and the internal audit function. The evaluation is performed by the Supervisory Board following its approval by the Management Board of the Bank and an opinion of the Audit Committee.

The evaluation of the adequacy and effectiveness of the internal control system is based on:

1) Internal Audit Department's annual report containing, among others, an evaluation of the adequacy and effectiveness of the internal control system and the risk management system,
2) Non-financial Risk Management Department's annual report on the effectiveness of the control function and quarterly reporting on critical and significant irregularities,
3) Compliance Department's annual report on the management of compliance risk in the Bank;
4) information of the Management Board of the Bank on the performance of tasks assigned to it within the internal control system,
5) information obtained from the parent company and subsidiaries, relevant to the adequacy and effectiveness of the internal control system,
6) findings of the statutory auditor,

7) annual Supervisory Review and Evaluation Process (BION) performed by the KNF,
8) findings of control authorities,
9) evaluations and opinions of third parties, relevant to the adequacy and effectiveness of the internal control system.