

INTERNAL CONTROL SYSTEM OF SANTANDER BANK POLSKA

As required by the Statutes, the Bank operates an internal control system which supports the decision-making processes and contributes to the Bank's efficient operations, compliance with risk management rules, reliability of financial reporting as well as compliance with the law, international standards, internal regulations and best practice.

The internal control system covers the control function, compliance unit and an independent internal audit unit.

The internal control system addresses, among others, compliance with the requirements of the Sarbanes-Oxley Act, Volcker Rule (section 619 of the Dodd-Frank Wall Street Reform and Consumer Protection Act), requirements of RDA/RRF (Basel Committee on Banking Supervision 239: Principles for effective risk data aggregation and risk reporting), the requirements of Recommendation H (KNF) and Regulation of the Minister of Finance, Funds and Regional Policy of 8 June 2021 on the risk management system, the internal control system and remuneration policy at banks.

▪ OBJECTIVES OF THE INTERNAL CONTROL SYSTEM

The Bank ensures delivery of the Internal Control System objectives by means of relevant controls adapted to the specific nature of the particular area of the Bank's operations, the flow and complexity of processes, any attendant risks and the degree and severity of irregularities, effectiveness of IT systems supporting those processes, availability of human resources and the oversight exercised.

The aim of the Internal Control System is to ensure:

- a) effective and efficient operation of the Bank
- b) reliable financial reporting
- c) compliance with the risk management principles at the Bank
- d) compliance of the Bank's business with laws, internal regulations and market standards.

As part of the general objectives of the Internal Control System, the Bank defines specific objectives which are linked to the processes delivered at the Bank. While defining specific objectives of the Internal Control System, the Bank takes into account the following aspects:

- a) the scope and complexity of the Bank's operations;
- b) the scope of application of specific legal provisions, market standards and internal regulations which the Bank is obliged to observe;
- c) the extent to which the Bank's operational and business plans have been achieved;
- d) completeness, correctness and complexity of accounting principles;
- e) quality (accuracy and reliability) of the accounting, reporting and operational system;
- f) adequacy, functionality and security of the ICT;
- g) the Bank's organisational structure, breakdown of competences and terms of coordination of activities between the respective organisational units, sections and posts, as well as the system of documents and information creation and circulation;
- h) the scope of activities outsourced by the Bank to third parties and their impact over the effectiveness of the Internal Control System at the Bank.

The Internal Control System has five inter-connected components:

- a) control environment – organisation, process management, ethical values and competencies of employees that impact the control awareness;
- b) risk assessment – actions taken to identify and assess the materiality of the risks associated with the achievement of the Bank's objectives;
- c) control activities – actions and procedures aimed at implementation of the management guidelines and mitigation of the risk that may impede successful delivery of objectives;
- d) information and communication – a procedure designed to define, capture and communicate, in a relevant form and timely manner, the information that helps the staff to fulfil their roles effectively;
- e) monitoring – measures taken to evaluate the Internal Control System over time.

▪ ROLES IN THE INTERNAL CONTROL SYSTEM

The Supervisory Board oversees the implementation of an appropriate and effective Internal Control System. Each year, the Supervisory Board assesses the Bank's internal control system which is adequately adjusted to the Bank's organisational structure, risk management system and the size and complexity of the Bank's business. It covers all units across the Bank as well as its subsidiaries. The internal control system covers all significant controls, including those related to reporting and the Bank's operational activity.

As part of its supervision over the Group's operations, the Supervisory Board monitors the effectiveness of the Internal Control Systems based on the information obtained from the compliance unit, internal audit unit, the Bank's Management Board and the Audit and Compliance Committee.

The Supervisory Board approves the criteria for the adequacy and effectiveness of the Internal Control System and performs its annual assessment, also taking into account the responsibilities of the Bank's Management Board regarding the Internal Control System.

The Supervisory Board appointed the Audit and Compliance Committee to assist the Supervisory Board in fulfilling its oversight responsibilities to shareholders and other stakeholders in relation to:

- a) the quality and integrity of the accounting policies, financial statements and disclosure practices;
- b) compliance of the Bank's business with laws and internal regulations;
- c) independence and effectiveness of activities undertaken by internal and external auditors;
- d) the assessment of the effectiveness of the system of internal control and management of financial and non-financial risks.

The Risk Committee and the Audit and Compliance Committee are updated on a regular basis on the operation of the internal control system from the units of the second and third lines of defence which facilitates the on-going monitoring of the system's effectiveness.

The control findings are taken into account and used to improve the existing processes and safety by making relevant changes to internal processes and regulations. These are regularly verified by the Internal Audit Area.

The Audit and Compliance Committee is informed about the results of assessing the risk of failure to comply with the overall internal control targets.

The Management Board is responsible for developing and implementing the internal control system and ensuring that an adequate and effective internal control system is in place at all operational units, including subsidiaries, updating documented procedures of the internal control system as well as establishing the adequacy and effectiveness criteria for assessing the internal control system. The Management Board of the Bank is also responsible for overseeing the effectiveness of the Internal Control System, improving it and adapting to the level of risk related to the operations of Santander Bank Polska Group, business environment and malfunction of systems and processes.

The Management Board of the Bank is responsible for establishing a matrix of control functions and defining actions aimed at ensuring its application. The Control Function Matrix is a tool implemented in accordance with KNF's Recommendation H that outlines the Bank's relevant processes, linking them to the general and specific objectives of the internal control system and the key controls and checks for horizontal and vertical monitoring.

The Bank's Management Board is also responsible for appointing individuals in charge of interim, at least annual, review of internal controls and procedures in the Bank and for determining relevant remedial measures to remove deficiencies identified by the Internal Control System, and at least once a year informs the Supervisory Board about:

- a) the process of designing, developing and implementing an adequate and effective internal control system in all organisational units, ensuring the achievement of the underlying objectives;
- b) the scale and nature of significant and critical deficiencies and the most important mitigating actions aimed at removing these deficiencies, including corrective and disciplinary measures taken. The corrective measures include designing new and updating existing control mechanisms (e.g. change of procedure, training).

▪ **THREE LINES OF DEFENSE**

The internal control and risk management systems are based on three lines of defence (LoD). Control measures under the first line of defence check compliance with procedures and they are an ad hoc response to any identified deficiencies or shortcomings.

The first line of defence is focused on the management of risks in the Bank's operational activity and is based on business units which, as part of their day-to-day activities, generate risks that affect the achievement of the Bank's objectives. The first line includes activities performed by each employee to ensure the quality and correctness of the tasks completed. The first line of defence checks adherence to the procedures and responds to any identified irregularities.

Any significant and critical deficiencies detected by the first line of defence are immediately reported to the organisational unit of the second line of defence responsible for independent monitoring of the process in which that significant or critical deficiency was identified, and to the internal audit unit. Any critical deficiencies are also reported to the Management Board.

The second line of defence is formed by specialist units performing control functions which support the Bank's management in risk identification and management and provide assessment of the first line controls.

The key units of the second line of defence are as follows:

- 1) The Internal Control Model function at the Bank is performed by the Operational Risk Management and Internal Control Department (part of the Risk Management Division), whose responsibilities include but are not limited to:
 - a. confirming the adequacy and effectiveness of the Internal Control System with regard to ensuring the achievement of the objectives of the internal control system (including with respect to the results of vertical testing of compliance with key controls);
 - b. indicating significant and critical deficiencies at the Santander Bank Polska Group level identified during certification of the control model, as well as implementation of action plans, including reporting on measures taken to mitigate operational risk;
 - c. reporting the results of an analysis of impact of the relevant recommendations from internal and external audit, reports by supervisors and operational risk instruments (including metrics, scenarios, events and RCSA, control function matrix), and analysis of internal and external factors (technological, regulatory and organisational changes, etc.) on the Internal Control System;
 - d. supporting analyses of controls in cooperation with the compliance function, internal audit and specialist control functions (first line of defence).

- 2) the Financial Accounting and Control function that supports the Bank's management through assuring correct and reliable reflection of the Bank and Santander Bank Polska Group's standing in (internal and external) financial disclosures.
- 3) Compliance function, whose purpose is to support Santander Bank Polska Group's management in managing compliance risks to ensure that the Group complies with legislation, regulatory requirements and best practices, having regard to the fact that the compliance function is independently responsible for controls safeguarding compliance with legislation, internal regulations and market standards related to the type of business.

The responsibility for ensuring compliance in specialist areas, such as, inter alia, prudential rules, taxation, company law, employment law and health and safety, is allocated to the appropriate specialist function;

- 4) Risk Management function, whose role is to provide assurance that the key risks are being identified and managed by the management, and that the Bank acts in line with internal risk policies. The units of the Risk Management function support the Bank's management in the process of identifying and managing risk by providing relevant tools for risk management, monitoring and reporting.

Dedicated functions for independent risk management, including the Control Centre.

Operational rules and areas of responsibilities of the units forming the second line of defence are presented in detail in internal regulations, which take into account segregation of duties.

Significant and critical deficiencies detected in the second line of defence are immediately reported to the internal audit unit. Critical deficiencies are also reported to the Management Board and the Supervisory Board (Audit and Compliance Committee).

The third line of defence is the Internal Audit Area, whose activity is supervised by the Audit and Compliance Committee of the Supervisory Board.

The Internal Audit Area provides independent and objective examination and assurance on the first and second tier controls and the Bank's management system, including with regard to the effectiveness of managing the risk related to the Bank's business.

Critical deficiencies identified by the internal audit unit are reported to the Bank's Management Board and the Supervisory Board or the Audit and Compliance Committee. Critical deficiencies identified by the first line of defence are presented – by the decision of the head of the internal audit – to the Supervisory Board or the Audit and Compliance Committee.

Critical deficiencies detected in the third line of defence are immediately reported to the Bank's Management Board.

■ COOPERATION BETWEEN LoD FUNCTIONS

All three lines of defence co-operate closely by exchanging information about the dates, scope and results of checks/audits.

All organisational units of the Group's first line of defence have to co-operate with the second- and third-line defence units and specifically have to provide them with access to any information, documents, papers, systems, physical rooms, opinions and explanations from employees required to carry out checks/audits.

The audited units with identified deficiencies must develop and effectively implement mitigating actions in line with the agreed schedule.

▪ **THE RULES FOR ASSESSMENT OF THE EFFECTIVENESS AND ADEQUACY OF THE INTERNAL CONTROL SYSTEM BY THE SUPERVISORY BOARD**

The principles of classifying deficiencies detected by the Internal Control System are approved by the Bank's Management Board and the Supervisory Board.

The following categories of deficiencies are distinguished:

- a) Control/ task/ function deficiency: weakness of a control/ task/ function linked to residual risk assessed as very low, low or medium.
- b) Significant deficiency of a control/ task/ function is a weakness of that control/ task/ function which:
 - is connected with a high residual risk mitigated by a single control where a deficiency has been identified, or
 - relates to high-priority internal audit recommendations connected with a key control or Special Monitoring Controls (a special category of controls that are significant from the point of view of the entire Banco Santander Group).
- c) Critical deficiency (material weakness as defined by the Group) of a control/ task/ function: a weakness linked to a critical residual risk and communicated to the shareholders.

The Supervisory Board assesses the adequacy and effectiveness of the control function, the compliance unit and the internal audit unit, taking into account in particular:

- a) the information from the Bank's Management Board on the manner of discharging duties related to the Internal Control System;
- b) periodical reports of the compliance unit and internal audit unit;
- c) information significant in terms of the adequacy and effectiveness of the Internal Control System, obtained from Santander Group and subsidiaries;
- d) findings of the certified auditor;
- e) findings of audit and control activities carried out by authorised institutions;
- f) any reviews and opinions issued by third parties which are significant from the point of view of adequacy and effectiveness of the Internal Control System.