

Internal Systems Governance

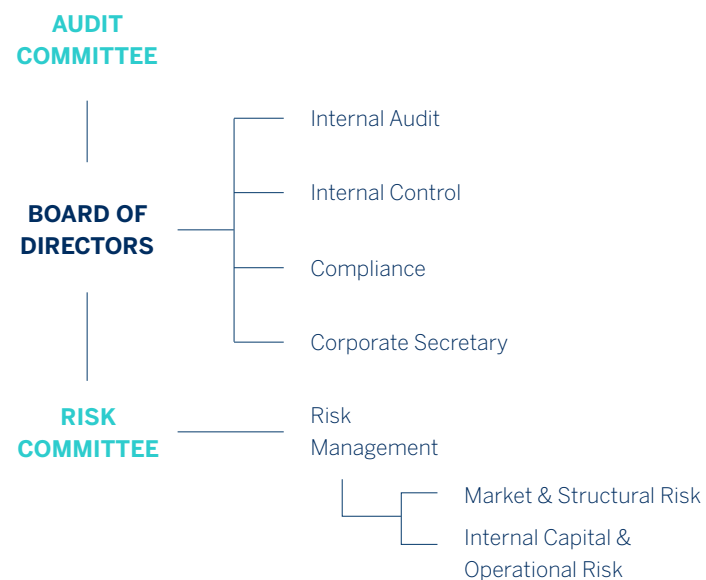
2,054 8 min 4 internal

The Risk Committee is constituted by the members of the Board of Directors, and is responsible for overseeing risk management policies and practices, their alignment with strategic goals, capital adequacy and planning, and liquidity adequacy, as well as the management's ability to assess and/or manage various risks inherent in the operations.

Risk Management is composed of the Internal Capital and Operational Risk Department and the Market and Structural Risk Department under the execution and management of the Head of Risk Management, and Validation, Credit Risk Control and Risk Management Control functions.

The responsibilities of the Head of Risk Management are outlined below:

- Ensure that risk management culture is recognized and risk management principles are widely embraced throughout the Bank and its affiliates, and make sure that an integrated risk management system is implemented which measures all of the Bank's risks collectively, which guarantees that limits determined in connection with the risk appetite approved by the Board of Directors are not breached, which is in compliance with applicable legislation, the Bank's strategies and policies, and which pursues risk-return relationship and entails control and validation activities,
- Define, measure, monitor and report risks, and ensure that all control activities are conducted thoroughly and timely; monitor and supervise results.



The responsibilities of the Internal Capital and Operational Risk Director are outlined below:

- Propose operational risk, reputation risk and risk appetite principles which are then set down by the Board of Directors,
- Ensure that all operational risks are covered by the first and second lines of defense,
- Conduct measuring, monitoring and analysis activities for risk appetite, operational risk, regulatory liquidity and regulatory capital adequacy; report their results regularly to relevant units, committees and senior management,
- Coordinate the ICAAP (Banks' Internal Systems and Internal Capital Adequacy Assessment Process) workflow,
- Oversee affiliates' adherence to Enterprise Risk Management Framework.

The responsibilities of the Market and Structural Risk Director are outlined below:

- Propose market, counterparty credit, liquidity, structural interest rate and exchange rate risk principles which are then set down by the Board of Directors; review and update the same,

- Carry out risk-based measuring, modeling, monitoring and analysis activities; report their results regularly to relevant units, committees, and senior management,
- Perform market, counterparty credit, structural interest rate, exchange rate and liquidity risk-based activities within the scope of ICAAP, stress testing and risk appetite framework, and risk assessment for new business and products/services; monitor and report risk-based concentrations,
- Monitor affiliates' adherence to Enterprise Risk Management Framework.

THE INTERNAL AUDIT DEPARTMENT

The activities of the Internal Audit Department are planned and executed with the aim of providing reasonable assurance about the effectiveness of risk management and control systems.

Multi-year audit plans are prepared according to the priorities that are defined in line with this aim. The scope and priority of on-site and remote audits to be conducted are determined based on the results of continuous risk assessments. The dynamic planning made ensures a thorough and continuous oversight of the main risk exposures of all business lines and subsidiaries, and the domains and focal points that are exposed to those risks. The audit scopes, quarters and the workforce to be allocated for audits are revised if deemed necessary according to the changes in risks.

The Internal Audit Department always aims to be a leader in realizing the best practices in internal audit. The Agile Methodology employed with a high maturity level in audit activities enables more efficient utilization of the workforce, enhanced risk-based approach, and production of high added-value results. It also allows uninterrupted continuation of the internal auditors' rapid adaptation to the post-Covid-19 new normal.

The Internal Audit Department carries out internal and external quality assurance studies in relation to its activities. Intensive and systematic finding follow-up is made to remediate the deficiencies reported by the Internal Audit Department. The role

of the Internal Audit Function as not only focusing on the past but also foreseeing potential risks and guiding the future becomes more and more prominent across the Bank. As part of this role, the Internal Audit Department also carries out advisory activities focused on various areas in addition to assurance audits. The Internal Audit Department uses data for all its activities and carries out most of the audits as focusing on the data. The team of auditors comprised of data scientists with modeling capabilities and data specialists with advanced data analysis capabilities is further strengthened by the day. Audit projects that employ advanced analytics and modeling such as machine learning, image processing and text mining are conducted successfully.

The Bank losses resulting from internal fraud continue to remain low. The use of artificial intelligence by the Internal Audit Department for fraud detection is among the pioneering practices in the sector. Internal fraud detection that relies on rule-based monitoring are backed by machine learning by using as basis the past incidents.

The Internal Audit Department supports the professional development of the auditors and encourage them to obtain professional certifications and to complete graduate and post-graduate programs. These efforts made in parallel with the Internal Audit Department's development and talent management strategies serve to increase the depth and quality of the audits performed.

THE INTERNAL CONTROL UNIT

The Internal Control Unit is responsible for the establishment and coordination of a sound internal control environment within Garanti BBVA. The Unit ensures that banking activities are carried out in accordance with the management strategies and policies in a regular, efficient and effective manner within the existing regulatory framework and guidelines.

Roles and responsibilities that are assumed within the scope of the Operational Risk and Control Model that is structured at the Bank according to the three lines of defense principle are fulfilled

by internal controllers who report to the Internal Control Unit. Accordingly, it is guaranteed that duties are separated functionally, powers and responsibilities are shared, a system of concurrence is established, risks exposed by business units are defined and quantified, and necessary controls are designed and carried out. Along the first line of defense, a structure that challenges the adequacy and quality of designed controls for business processes is operated with an approach that encompasses the Bank's all branches, regional offices and Head Office departments and financial subsidiaries.

Within this structure, inspection and control activities are conducted by means of on-site or remote control methods for the Bank's branches and regional offices, in addition to all Head Office departments. Besides control activities, assistance is lent to devising the training programs aimed at building on the operational risk awareness of the Bank's employees, some of which are delivered directly by internal controllers specifically to the employees working in branches.

Additionally, the IT Internal Control Function is also fulfilled, where IT Risk Control Specialists team set up under the Internal Control Unit oversees that the Bank's IT activities are carried out securely and within the rules defined by the Bank. A dedicated team coordinates the internal control teams assigned to financial subsidiaries and supervises that the Bank's norms are implemented consistently across all affiliates.

Findings and suggestions resulting from the activities are reported to relevant parties and necessary actions are followed up by systemic mechanisms and the Committees that make up the governance mechanism.

The Operational Risk Admission and Product Governance Committee Secretary that reports to the Internal Control Unit – Outsourcing Risks Team coordinates the process incorporating the definition of risk exposure resulting from new initiatives (business/product/service, process/technology transformations, and outsourcing including support/appraisal services), establishment of an effective control environment necessary to mitigate those

risks, and taking risk mitigation measures. In addition, service procurements that fall under support services regulation and risks and controls stemming from outsourcing are also considered and monitored by the Outsourcing Risks Team.

The Internal Control Unit is also responsible for verifying that the internal control environments of the Bank's financial subsidiaries are adequately outfitted in terms of structure and functionality. In this context, teams that are responsible for the control function serve at the relevant subsidiaries; internal control teams are assigned to ensure healthy operation of the control environment at the Bank's consolidated subsidiaries in accordance with the applicable legislation. Regular meetings are held with these teams, and related teams periodically report to the Internal Control Unit.

THE COMPLIANCE DEPARTMENT

Working with the purposes of managing the potential compliance risks of the Bank and of identifying and preventing these risks in advance, the Compliance Department aims to help improve the compliance culture constantly across the Bank. The Compliance Department carries out the following tasks.

The Compliance Officer Team performs the following duties:

- Carry out all necessary efforts to achieve the Bank's compliance with the regulatory framework concerning prevention of money laundering and countering the financing of terrorism, and provide necessary coordination and communication with the Financial Crimes Investigation Board (in Turkish: MASAK),
- Supervise the compliance of the companies within Garanti BBVA financial group that are obliged to achieve compliance with the MASAK legislation,
- Ensure that the Financial Group Compliance Program and the Bank Compliance Program which is prepared in harmony with the former are executed; prepare and conduct sub-policies and procedures accordingly,
- Prepare the annual training program on anti-money laundering and countering financing of terrorism, and follow-up its implementation,

- Looks into and evaluate information on potentially suspicious transactions that it receives or becomes aware of; report any transaction that it deems to be suspicious to the Financial Crimes Investigation Board (MASAK),

In terms of compliance activities regarding customer products and services, assessments are made on the compliance of products and processes to applicable regulations. Activities are carried out in relation to compliance controls in accordance with the Regulation on the Internal Systems and Internal Capital Adequacy Assessment Process of Banks. The control mechanisms in place are monitored with respect to compliance of the Bank's current and planned activities, new transactions and products with the laws and the Bank's policies. The processes are monitored for any necessary revisions according to regulatory changes, related employees are notified on such changes.

As part of corporate compliance activities, the Compliance Department is responsible for promoting awareness of Code of Conduct, Anti-Corruption Policy, and Competition Policy, encouraging due execution of these policies, ensuring development and dissemination of the procedures for execution, and offering advisory for resolving any hesitations that may arise during the implementation of the policies and procedures. The Compliance Department also manages the Whistleblowing Channel, which is generally used to report any noncompliance to Code of Conduct. In the process where the identity of the person who reported is kept confidential, all reports received are processed carefully and promptly, ensuring they are investigated and resolved.

Securities compliance activities encompass examination of suspicious transactions within the scope of the Capital Markets Board (CMB) Communiqué on Obligation of Notification Regarding Insider Trading and Manipulation Crimes. Procedures are established regarding own-account trading and use of privileged information by the Bank or subsidiary employees who may have insider information or periodic information about capital market instruments or issuers in connection with the

performance of their jobs. In addition, relevant legislation and internal guidelines are also followed up.

The Compliance Department also monitors the compliance activities at the Bank's affiliates and overseas branches. In this respect, personnel responsible for the compliance function are assigned at affiliates and overseas branches. Compliance activities and potential risks are supervised regularly through regular meetings and periodic reports.

The activities carried out for achieving compliance with the legislation on the Protection of Personal Data are also coordinated by the Compliance Department. In this context, the Department directly supports the related departments for ensuring that personal data are processed in accordance with the legislation, possible data breaches are prevented, processes are designed in line with this goal and with the legislation, and necessary technical and administrative measures are taken.

The Assurance Function set up under the Compliance Department carries out specific control activities and inspections on process that compliance risk at the Bank and its affiliates according to risk assessment results, and evaluates the adequacy of the control mechanisms in place.

In performing all of its duties and responsibilities outlined above, the Compliance Department continues to work in coordination primarily with the Internal Audit Department, Internal Control Unit, Training Department, Customer Security and Transaction Risk Management Department, Legal Department and Customer Experience Management Department, as well as other relevant units.