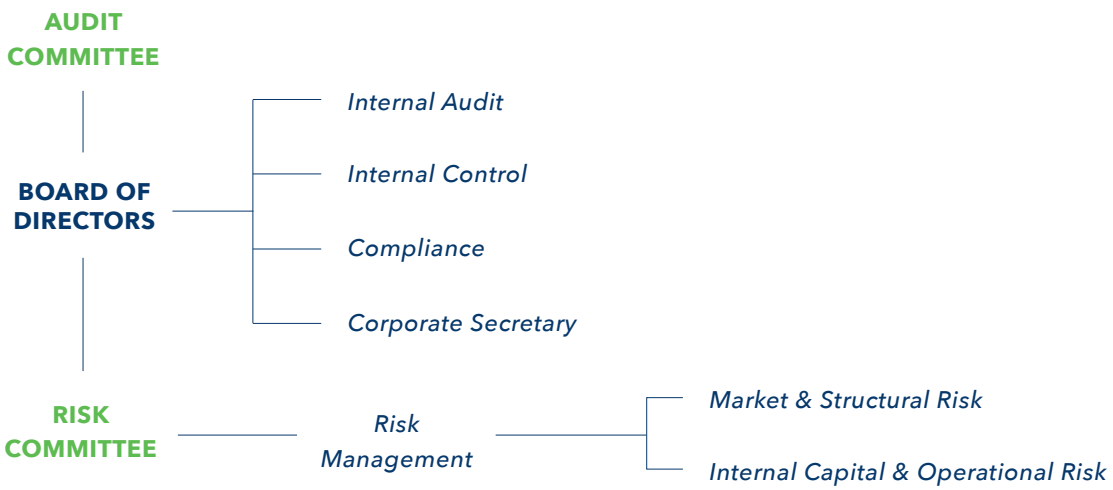
Internal Systems Governance

2,968 15 min 6 risk



The Risk Committee is composed of 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 Internal Capital and Operational Risk Department and 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 INTERNAL CAPITAL AND OPERATIONAL RISK DIRECTOR ARE OUTLINED BELOW:

→ Propose operational risk, operational risk admission 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, operational risk admission and 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 Corporate Risk Management Framework; ensure that an infrastructure for defining, measuring, monitoring and controlling risks is in place.

THE RESPONSIBILITIES OF 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, 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; ensure that an infrastructure for defining, measuring, monitoring and controlling risks is in place.

THE INTERNAL AUDIT DEPARTMENT

The Internal Audit Department adopts a risk oriented approach and performs a comprehensive risk assessment that covers the Bank and all its subsidiaries and prepares an annual audit plan in line with the Bank's goals and strategic priorities and taking into consideration the expectations of all stakeholders including especially the Board of Directors. The "continuous risk assessment" approach ensures seamless monitoring of the changes in risks and allows dynamic planning.

Keeping a close eye on the new approaches and current trends in the banking industry and internal audit field, the Internal Audit Department expanded the Agile Methodology that it adopted starting from 2019 to all of its audits in 2020. The Agile Methodology implemented serves to attain higher productivity from the workforce, produce high added-value results, and improve communication with the auditees.

The checklists of the audits performed in accordance with the agile methodology are designed with a value-focus and constant value creation is put in the focal point by making sure that the audit subjects that create the maximum value are addressed in the initial stages of the audits. Each audit in the audit plan is handled as an individual project; audits are divided into two-week sprints and the results from each sprint are shared following the sprints with the auditees, without waiting for the end of the audit, thereby securing fast actions for remediating the findings. In addition, implementation planning for actions is made with the auditees at the management level at the end of each sprint.

Continuous risk assessment, the flexibility afforded by the agile methodology, strong communication with the auditees and value-focus allow the Internal Audit Department to quickly adapt to the new normal resulting from COVID-19. Since day one of the COVID-19 precautions, consultancy is offered for managing the risks stemming from the pandemic, and risk assessments are updated so as to enable changes in the audit plans specifically for the emerging new risks. In addition, the Agile Methodology guarantees no setbacks in the achievement of performance targets by units even during periods of remote working-.

Dedicated systems are used to oversee the processes of audit planning, field work execution, preparation of an audit report regarding identified deficiencies and monitoring and reporting of the findings. While Microsoft Office applications are used in the planning, field and reporting processes of audit activities that are conducted based on risk types, data inquiry and processing software such as Oracle Business Developer and SQL Developer are employed for areas requiring data analysis.

Data scientists are employed with the aim of adopting a data driven approach to audit processes to minimize the increased technological and cybersecurity risks in line with the Bank's digital transformation target. These advanced data inquiry and big data analysis capabilities enable audits that rely on machine learning technology. At least one data specialist is assigned to each audit and data scientists perform studies aiming to enhance the quality of operational efficiency and audit results through specific projects concentrated on machine learning. Hence, an audit methodology that relies on the examination of the data universe instead of examination based on sampling is adopted in audit processes with the target of minimizing audit risks and increasing confidence interval.

The Internal Audit Department performs risk-based process audits in 11 main risk areas of the Bank by covering head office units, domestic branches, foreign branches and subsidiaries.

Within the scope of **BUSINESS MODEL RISK**, focus is placed on business model viability, business model sustainability, pricing and other aspects of strategy.

Within the scope of **CORPORATE GOVERNANCE AND RISK MANAGEMENT RISK**, audits are conducted in relation to risk management and risk control framework, as well as audits of organizational framework such as corporate policies, procedures, duties and responsibilities.

Within the scope of **CAPITAL RISK**, audits are performed in relation to evaluation of the control environment within the scope of regulatory and internal capital computations and capital adequacy assessment, compliance with the legislation, policies and procedures, and accuracy of calculations.

Within the scope of **CREDIT RISK** audits, credit risk, thresholds and limit structure, loan portfolios and credit processes that have been established are audited.

Within the scope of **MARKET RISK**, assessments are made to determine the risk of loss that the Bank's on and off-balance sheet positions may be exposed to within the frame of exchange rate, commodity and interest rate risks resulting from the movements in market prices.

Within the scope of **STRUCTURAL RISK**, audits are conducted in relation to assets and liabilities management model and validation, structural risk stress test, liquidity risk stress test, financial institutions borrowing instruments and treasury reporting processes.

Within the scope of **OPERATIONAL RISK**, audits are conducted in relation to operational processes with a particular focus on processes, products and services that are either revised by the Bank or are offered as new services, as well as to digital channels enterprise and data governance.

Within the scope of **LEGAL RISK**, audits are conducted regarding regulations governing financial reporting, litigation, compliance with binding instructions, and the risks with a potential negative impact on financial statements.

Within the scope of **COMPLIANCE RISK**, focus is placed on audits regarding reputational risk management, as well as potential risks that may arise from non-compliance with ethical standards and legal regulations such as prevention of money laundering and countering financing of terrorism, customer and investor protection and personal data protection.

Within the scope of **TECHNOLOGY RISK** audits, the adequacy and effectiveness of the internal control environment established by the Bank for risks stemming from its use of technology are assessed. Accordingly, audits are conducted with a focus on cybersecurity, information security, IT operations, and business continuity.

Within the scope of **EXTENDED ENTERPRISE RISK** audits, audits are conducted on various processes such as service or product and construction management, as well as audits of support services providers, the scope of which has been set by the BRSA (Banking Regulation and Supervision Agency).

Within the scope of the inspections and investigations among the activities of the Internal Audit Department, fraudand counterfeiting activities are prevented or detected, upon which necessary managerial actions are taken promptly. Remote and on-site studies are carried out to determine internal fraud incidents.

The audit activities on the basis of risk types mentioned above are mainly performed by auditors specialized in the related risk area. Parallel to the development and talent management strategies of the Internal Audit Department, risk-based specialization approach to audit combined with the constant encouragement of academic education and professional certification processes aimed at building on the theoretical and professional knowledge and skills of auditors result in increased technical depth of the audits performed.

All findings resulting from the audits conducted by the Internal Audit Department are continually followed up. Regular information flow to management aimed at speeding up continuous finding monitoring and remedy processes and ensuring timely actions are intended to remedy all findings in a timely manner.

All activities of the Internal Audit Department are continuously monitored via internal and external quality assessments.

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.

Within the applied internal control model that is structured according to three lines of defense principles, controls are identified by the first line of defense teams in the business units by taking the relevant risks into consideration. There is a process in place whereby the results of control activities are reported from business units to the relevant second line of defense functions. In this model, the Internal Control Unit ensures the proper execution of control activities performed within the Bank by implementing a common methodology. On-site and remote control activities are carried out regarding the branches (including foreign branches) and Regional Offices. Regarding the Head Office departments, the related control activities which are regularly conducted within the business/support units are monitored closely and challenged and verified in order to ensure their timely, thorough and accurate performance.

The IT Internal Systems Control team, set up within the Internal Control Unit, oversees the secure performance of IT functions in accordance with the guidelines set by the Bank. The team defines internal control steps for IT processes, and subjects them to control activities in accordance with predefined control items, methodology and tools. In addition, they carry out process reviews to determine technology risks and closely monitor studies to eliminate identified deficiencies.

The Internal Control Unit is also responsible for supervising that the internal control environments of the Bank's financial subsidiaries are adequately outfitted in terms of structure and functionality.

Findings and recommendations resulting from control activities are reported to relevant managerial levels and agreed actions are followed up.

Moreover, the Internal Control Unit offers training programs for increasing risk/control awareness of the Bank's employees and provides them with the necessary guidance.

THE COMPLIANCE DEPARTMENT

Working with the purposes of managing the potential compliance risks of the Bank and of identifying and preventing these risks before implementation, the Compliance Department aims to help improve the compliance culture

constantly and establish a world-class compliance culture across the Bank. The Compliance Department carries out the following tasks.

The Compliance Officer Team performs the following duties as also stipulated by the regulations governing prevention of money laundering and countering the financing of terrorism:

- Carry out all necessary efforts to achieve Garanti BBVA's compliance with the regulations issued to prevent money laundering and countering the financing of terrorism and provide necessary coordination and communication with the Financial Crimes Investigation Board (in Turkish: MASAK),
- Ensure that the Compliance Program is carried out; develop policies and procedures within this scope; execute risk management, monitoring and control activities; follow up the results of internal audit and training activities,
- Lay down the efforts related to the training program about prevention of money laundering and countering the financing of terrorism for the approval of the Board of Directors, and ensure that the approved training program is carried out effectively,
- Look into and evaluate information on potentially suspicious transactions that it receives or becomes aware of sua sponte; report any transaction that it deems to be suspicious to the Financial Crimes Investigation Board,
- Manage relations with relevant governmental or private agencies.

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 requirements of Article 18 of the Regulation on the Internal Systems and Internal Capital Adequacy Assessment Process of Banks. The control mechanisms in place are monitored and coordinated with respect to compliance of the Bank's current and planned activities, new transactions and products with the laws, internal policies and guidelines, and banking practices. The processes are monitored for any necessary revisions according to regulatory changes, related employees are notified on such changes, and opinions are formed prior to introduction of new products and transactions.

As part of corporate compliance activities, the Compliance Department is responsible for promoting awareness of "Garanti BBVA Code of Conduct" approved by the Board of Directors in 2015, "Anti- Corruption Policy" approved in 2018 and "Competition Policy" approved in 2019, encouraging adherence to the documents, ensuring development and dissemination of the procedures to be formed in the context of the documents, and helping resolve any doubts that may arise during the interpretation of the documents. These documents are available on the Intranet accessible to all employees and training sessions are organized during the course of the year.

In addition, Garanti BBVA Code of Conduct, Anti-Corruption Policy Statement and Garanti BBVA Competition Policy are made public on the Investor Relations website. Detail information can be reached from the related links.

The Compliance Department manages the Whistleblowing Channel, which is established to report any noncompliance to Garanti BBVA Code of Conduct and forms an essential part of the compliance system. The channel is also a resource to assist the employees in reporting transgressions that they observe or which are reported to them by their team members, customers, suppliers or colleagues. Communications through this channel include, but are not limited to, the reporting of suspicious illegal conduct or professionally unethical conduct. In case of an actual or suspected breach of Garanti BBVA Code of Conduct, the incident is reported immediately via the Garanti BBVA Whistleblowing Channel, by e-mail at etikbildirim@garantibbva.com.tr or by telephone at +90 216 662 5156. The Compliance Department, responsible for managing the Whistleblowing Channel, processes all reports received carefully and promptly, ensuring they are investigated and resolved in accordance with the Whistleblowing Channel management procedures. The identity of the person who reported is kept confidential. The information is made known only to those departments whose cooperation is necessary for the investigation process.

The result of the investigation is communicated to the departments that need to take appropriate measures to correct the transgression, as well as to the person being reported and the reporter, as appropriate. Nobody, who reports any facts or activities through the Whistleblowing Channel in good faith, will be the target of reprisal nor will he/she suffer any other adverse consequence as a result. Garanti BBVA Code of Conduct also covers incidents of conflict of interest and aspects that would prevent employees' professional behaviors from being affected thereby.

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 being established regarding own-account trading and use of privileged information by the Bank employees who may have insider information or periodic information about capital market instruments or issuers in connection with the performance of their jobs, professions and tasks. In addition, relevant legislation and internal guidelines are also monitored.

With respect to subsidiaries' coordination activities, the Compliance Department monitors the compliance activities at the Bank's subsidiaries and overseas branches. In this respect, there are individuals assigned at subsidiaries and overseas branches who are responsible for the compliance function; in line with the related legislation, an employee is assigned at each of the consolidated subsidiaries and overseas branches for monitoring compliance with local regulations. Meetings are held regularly with the said employees who submit periodic reports to the Compliance Department.

Within the scope of Compliance Models and Assurance, compliance models and methodology are designed and implemented; risk assessment are carried out for all compliance specialization areas and risk monitoring methodology are created, implemented and measured. Furthermore, control activities of processes for managing compliance risk are carried out as part of the assurance activity.

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 and Legal Department, as well as other relevant units and people.