REGULATIONS OF THE INFORMATION TECHNOLOGY AND CYBER-SECURITY COMMITTEE OF BBVA'S BOARD OF DIRECTORS

The Board of Directors of Banco Bilbao Vizcaya Argentaria, S.A. ("BBVA", the "Bank" or the "Company"), in accordance with its Regulations, has resolved to set up a specific committee on information technology and cyber-security to assist the Board in the performance on matters within the scope of its powers (the "IT and Cyber-security Committee" or the "Committee").

Legal Nature

The IT and Cyber-security Committee is a body of the Board of Directors that has no executive powers and is governed by the Board Regulations and these Regulations.

Purpose

The purpose of the IT and Cyber-security Committee is to assist the Board of Directors in:

- the understanding and acknowledgment of the risks associated to technology and information systems related to the Group's activity and the oversight of its management and control, particularly with regard to the cyber-security strategy;
- the acknowledgment and supervision of the infrastructure and technology strategy of the Group and how this is integrated into the development of its overall strategy;
- ensuring that the Bank has determined plans and policies, and has appropriate means, for managing the above-mentioned matters;
- as well as in any other issues and responsibilities that may be attributed to the IT and Cyber-security Committee by the Board at any given time within this scope.

Composition

The IT and Cyber-security Committee will have a minimum of three members appointed by the Board among its directors, which will also nominate the Chair of this Committee. For this purpose, the Board will take into consideration the knowledge and experience in technology, information systems and cyber-security matters.

Rules of Organisation and Operation

The IT and Cyber-security Committee will meet as often as necessary to perform its duties, convened by its Chair or by whoever stands in for its Chair pursuant to these Regulations.

Should the Chair be absent, the meetings of the Committee will be chaired by the most long-standing member of the Committee and, in the event of more than one member of equal seniority, by the eldest.

The Committee may request the attendance at its meetings of persons with tasks within the Group that are related to the Committee's duties. The usual channel for a request of this nature will be through the reporting lines of the Company organisation, although, in exceptional cases, the request may be made directly to the person whose assistance is required.

In particular, the Committee will maintain a direct and recurring contact with the executives responsible for the areas of Engineering and Cyber-security in the Group, for the purpose of receiving the necessary information for a better performance of the Committee’s duties. This information will be discussed in the meetings held.

The Committee may also engage external advisory services as may be necessary to establish an informed opinion on matters related to its duties. This will be done through the Secretariat of the Board.

The system for convening meetings, quorums, the adoption of resolutions, minutes and other details of its operation will be in accordance with the provisions of the Regulations for the Board of Directors, insofar as they are applicable.

Functions

Within the purpose established in the relevant section of these Regulations, the IT and Cyber-security Committee shall perform the following functions:

Oversight of technological risk and cyber-security management

1. Review the major technology risks exposures of the Bank, including information security and cyber-security risks, and the steps management has taken to monitor and control such exposures.

2. Review the policies and systems for the assessment, control and management of the Group's technology risks and infrastructures, including the cyber-attack incident response and recovery plans.

3. Receive reports from management regarding the business continuity planning in technology and technology infrastructure matters.

4. Receive reports from management, as and when appropriate, on:

    a. IT-related compliance risks; and

    b. the steps taken to identify, assess, monitor, manage and mitigate those risks.

5. Additionally, the IT and Cyber-security Committee will be informed of any relevant event that may occur regarding cyber-security issues. These are deemed to be those which, individually or as a whole, may have a material impact or damage in the Group's equity, results or reputation. In any case, such events will be informed to the Chair of the Committee as soon as possible.

Stay informed of the Technology Strategy

6. Receive reports from management, as and when appropriate, on technology strategy and trends that may affect the Company's strategic plans, including the monitoring of overall industry trends.

7. Receive reports from management, as and when appropriate, on the metrics established by the Group for the management and control of IT-related matters, including the progress of the developments and investments carried out by the Group in this field.

8. Receive reports from management, as and when appropriate, on matters related to new technologies, applications, information systems and best practices that affect the Group's IT strategy or plans.
9. Receive reports from management on the core policies, strategic projects and plans defined by the Engineering area.
10. Inform the Board of Directors and, if applicable, the Executive Committee, on any IT-related matters falling within the scope of their functions.

For a better performance of its functions, channels for an appropriate coordination between the IT and Cyber-security Committee and the Audit and Compliance Committee will be established to ensure:

- That the IT and Cyber-security Committee can have access to the conclusions of the work performed by the Internal Audit Department in technology and cyber-security matters.
- And that the Audit and Compliance Committee is informed on IT-related systems and processes that are related to or affect the Bank's internal control systems and other matters falling within the scope of its functions.

Additionally, channels for an appropriate coordination between the IT and Cyber-security Committee and the Risks Committee will be established to ensure that the Risks Committee monitors the impact of technological risks within the scope of Operational Risk and other matters falling within the scope of its functions.