



# 03.5

## INTERNAL CONTROL AND COMPLIANCE

IN BANKIA THERE IS AN ONGOING  
COMMITMENT TO COMPLY WITH BANKING  
STANDARDS AND REGULATIONS.

The increasing complexity of the international, European and Spanish regulatory and supervisory rules to which financial institutions are subject has made internal control and compliance activities even more important and necessary, as more effective and efficient mechanisms of risk control and risk management.

In 2017 this demanding regulatory environment was further complicated by preparations for the entry into force of the new Markets in Financial Instruments Directive (MiFID II), the new Payment Services Directive (PSD2) and the General Data Protection Regulation (GDPR).

Bankia has an effective internal control and risk management organisation and effective systems to ensure compliance with the rules to which its actions are subject and with good banking practices.

### CRIMINAL RISK PREVENTION

Bankia's criminal risk prevention model identifies the activities that must be prevented and the necessary protocols and procedures to avoid any behaviour that could give rise to criminal liability. The model requires the implementation of controls (some general, others more specific, assigned to previously appointed officers) and adopts the rules of conduct set out in the bank's Code of Ethics and Conduct.

In line with the criteria set out by the Office of the State Public Prosecutor and with criminal liability prevention best practice, in 2017 Bankia engaged an outside expert to prepare an independent review report on the bank's criminal liability prevention model.

The bank has computer software that allows it to systematically map its criminal liability prevention risks and controls, so as to detect any circumstance that could entail an increased risk of the commission of criminal acts.

Additionally, in 2018 Bankia will adapt its criminal liability prevention model to the bank's new situation after the merger with BMN, updating the risk and control map.

## ANTI-MONEY LAUNDERING/ COMBATING THE FINANCING OF TERRORISM (AML/CFT)

Bankia collaborates actively with the institutions responsible for supervising and controlling compliance with European and Spanish laws and regulations on the prevention of the laundering of the proceeds of criminal activities and terrorist financing. For this purpose, Bankia has mandatory rules and procedures to:

- Ensure compliance with applicable AML/CFT laws and regulations and the recommendations of the national and international authorities.
- Assess the exposure to AML/CFT risk in its activity.
- Implement the necessary rules of conduct and control and reporting systems to prevent the bank from being used to launder money or finance terrorism.
- Establish customer acceptance and know-your-customer policies and ensure that all employees are aware of and adhere to them.
- Train all its employees in a culture of compliance aimed at delivering a good service to its customers.

*IN 2018 THE FOURTH EUROPEAN ANTI-MONEY LAUNDERING DIRECTIVE IS EXPECTED TO BE INCORPORATED INTO SPANISH LAW.*

**NO. OF EMPLOYEES TRAINED IN CRIMINAL RISK PREVENTION**

**53**

**NO. OF EMPLOYEES TRAINED IN THE PREVENTION OF MONEY LAUNDERING**

**1,518**

In 2018 the fourth European anti-money laundering directive is expected to be incorporated into Spanish law. This new directive affects, among other things, the maximum permitted amount of cash transactions and the possibility of information sharing between countries in order to more effectively combat money laundering, especially the financing of terrorism, as this is at the top of the European agenda after the multiple terrorist attacks perpetrated in 2017.

In the field of technology, in 2018 a series of technologies will gradually be introduced to improve customer knowledge and facilitate integrated prevention through data analysis and artificial intelligence.

# 03.5

## INTERNAL CONTROL AND COMPLIANCE

### DATA PROTECTION

Bankia has adopted a set of measures to ensure proper implementation of data protection principles and customers' data protection rights. The rules include instructions and provisions concerning the information that must be provided when collecting data, the duty of secrecy and custody of data, the need to obtain consent for data processing, and exercise of the rights of access, rectification, cancellation and objection.

Customer information is one of Bankia's most important assets and protection of that information is a priority, especially in view of the recent advances in technology and communication. As a financial institution at the service of the society that demands its services, the bank directly assumes a very substantial part of the responsibility for ensuring comprehensive security.



Bankia also has a legal and ethical obligation to protect, on the same terms, the information of collaborating entities, other persons with which the bank has dealings and official bodies.

During 2017, the group started a project to adapt to the new General Data Protection Regulation, which will come into force on 25 May 2018 and will affect the entire organisation. The aim is to analyse the possible legal, organisational and technological impacts of this new regulation and gradually take whatever steps or measures may be necessary in order to ensure compliance.

The main purpose of the General Data Protection Regulation is to implement common data protection principles, rules and standards (rights of data subjects and obligations of data controllers) that are adapted to the digital environment. The new regulation represents a substantial change compared with the previous regulation and is a challenge for the bank.

*IN 2017 THE GROUP STARTED A PROJECT TO ADAPT TO THE NEW GENERAL DATA PROTECTION REGULATION, WHICH COMES INTO FORCE IN 2018.*

## THE CHALLENGES OF MiFID II

The prospect of the entry into force of the second Markets in Financial Instruments Directive (MiFID II) in 2018 forced the bank to make considerable efforts during 2017 to analyse and adapt both its processes and procedures and its business model. The aim is to improve the advice given to customers and to design and distribute investment products and services that match customers' needs and interests.

Important changes in MiFID II include a strengthening of the conduct of business rules, already regulated by MiFID I, that are to be applied when providing investment services, so as to offer greater investor protection.

The most noteworthy steps taken in 2017 to adapt to MiFID II, which will have to be consolidated in the course of 2018, are as follows:

- **Product governance.** The suitability and appropriateness assessments were reinforced in order to enhance customer knowledge and thus provide a more complete service, tailored to customers' needs, ensuring that those needs are met both in the design and in the distribution of investment services and financial instruments.
- **Continuous development of employees.** Bankia started specific training plans for employees in the commercial network to ensure that both the information about financial instruments provided to customers and the advice the customers are given result in a better service.
- **Greater information transparency.** The customer notification procedures were reinforced. The purpose is to provide customers with relevant and timely information on investment strategies and financial instruments and the associated costs and expenses.

At the same time, the entry into force of MiFID II makes it necessary to reinforce the information systems, as the new regulation requires banks to record large amounts of information. For example, MiFID II requires the recording of all relevant telephone conversations linked to transactions or to the provision of services that relate to the reception, transmission and execution of client orders.

During 2017, a total of 5,266 Bankia employees received training in MiFID II, of which 94.1% passed. Added to them are the 2,147 employees of BMN, with a pass rate of 71.5%.

As of January 2018, a total of 2,657 professionals had enrolled in the first phase of training. A total of 3,250 people are expected to enrol in the second phase.

# 03.5

## INTERNAL CONTROL AND COMPLIANCE

### INTERNAL CONTROL

The Corporate Internal Audit Directorate supervises and evaluates the effectiveness of the bank's corporate governance, risk management, internal control and information systems and also verifies compliance with internal and external regulations.

The directorate reports periodically to the Audit and Compliance Committee and to the bank's Senior Management on the implementation and results of the Annual Audit Plan and any audit recommendations and their degree of implementation. This reporting obligation is fulfilled through quarterly presentation of the Audit Follow-Up Report to the Audit and Compliance Committee and the Management Committee.

The Internal Audit function covers all the activities carried out in the group and has unlimited access to the information it needs for the performance of its tasks. In carrying out its work it may contact and gather information from any senior manager or employee of the bank. Internal Audit also participates actively in several of the group's control committees, including the Regulatory Compliance Committee,

the Ethics and Conduct Committee, the Operational and Technology Risk Committee, the Regulatory Monitoring Committee, the Anti-Money Laundering Committee and the Provisioning Committee.

Internal Audit has established seven processes, which summarise the work it does:

1. Preparation of the Audit Plan.
2. Execution of business centre audits.
3. Execution of process, centre and system audits.
4. Monitoring of audit recommendations.
5. Development and maintenance of audit function support applications.
6. Internal audit communication and reporting.
7. Collaboration with and coordination of external audits.

In recent years the Corporate Internal Audit Directorate has also developed various web applications designed to optimise its operations, such as the application that allows more agile communication between auditors and audit subjects.

AUDITS OF PROCESSES, PRODUCTS AND CENTRES	277
BRANCH AUDITS PER AUDIT PLAN	951
FRAUD PREVENTION ALERTS	1,125

## INFORMATION SYSTEMS

The Bankia Group is in the process of implementing a new information governance model. This is a far-reaching, enterprise-wide transformation project that encompasses all corporate information in the regulatory, analytical, commercial and risks areas.

The goal is to move towards a governance model that will turn information into a strategic asset and align the bank with best market standards, while also complying with the Basel Committee on Banking Supervision's standard on risk data aggregation (RDA).

The project comprises three lines of action:

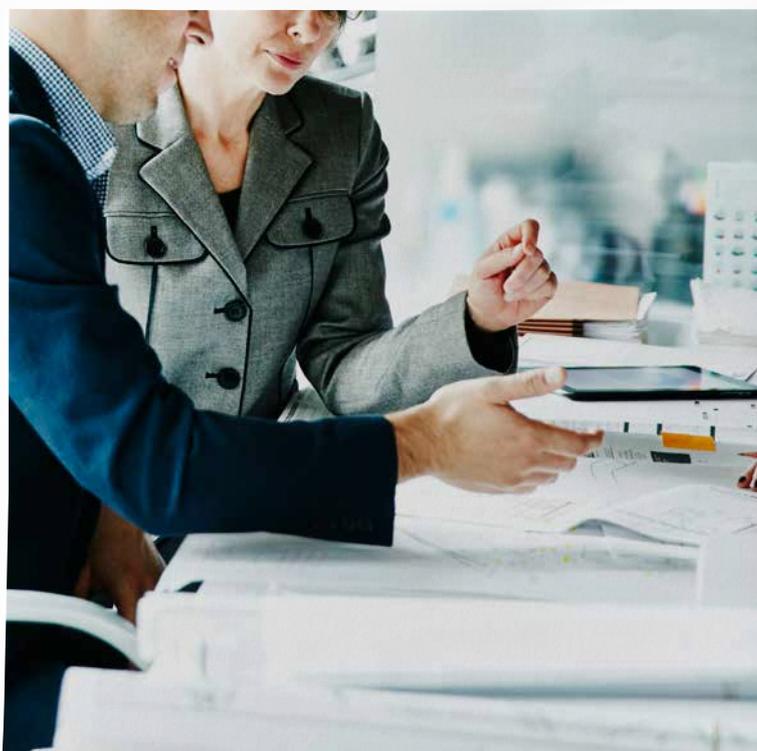
- Organise information through a single data repository and a common data dictionary.
- Optimise data provisioning and ensure consistency and flexibility in data use.
- Implement an information quality governance and control model throughout the data life cycle.

In 2017 the project progressed in the following aspects:

- Approval of the Regulatory Framework for Data Governance and Quality.
- Implementation of the first management reports with advanced visualisations (iPads, new reports on the SIG management information system platform).

- Construction of an in-house tool for mining regulatory financial statements that will allow functional users to validate and analyse their information more flexibly and dynamically.
- Report on the first regulatory statements from the new informational architecture.
- Registration of the first group of business concepts in the Single Glossary of Terms, which will assist user understanding.
- First dashboard for monitoring data quality.
- Definition of an overall data quality plan that will serve to gradually strengthen the various control points and ensure continuous improvement of information.
- Execution of the lines of work identified in the RDA Master Plan, which is designed to prepare the bank to be RDA compliant by December 2018. In 2013 the Basel Committee on Banking Supervision published a report containing a set of principles whose purpose is to strengthen banks' risk data aggregation capabilities and internal risk reporting practices.

In January 2019, institutions classified as Domestic Systemically Important Banks (D-SIBs), of which Bankia is one, must demonstrate to the banking supervisor that they properly comply with those principles, in other words, that the information on which Senior Management bases its risk-related decisions is properly governed, is sufficient and is of a reasonable quality.



# 03.5

## INTERNAL CONTROL AND COMPLIANCE

*BANKIA IS A MEMBER OF THE  
LARGE BUSINESSES FORUM,  
WHICH PROMOTES CLOSER  
COLLABORATION WITH THE  
SPANISH TAX AGENCY.*

### POLICY TAX

Responsible tax management, fraud prevention and detection, and tax transparency are principles that help ensure the bank's effective, sustainable development and build trust among stakeholders.

To safeguard these principles, Bankia adopts specific tax risk management and control measures. It also has internal control systems in place and has policies that establish the proper way to act in various areas, including corporate tax policy and tax risk management, transparency, corporate responsibility and good corporate governance.

The Board of Directors sets tax strategy, approves the risk policy, including the policy on tax risks, supervises internal reporting and control systems, approves investments that entail special tax risk and authorises the creation of, or acquisition of interests in, entities domiciled in tax havens.

The Audit and Compliance Committee, for its part, supervises the tax risk management system and reports to the Board on interests in entities domiciled in countries or territories that are considered tax havens.

The tax principles governing Bankia's activity are as follows:

- **Transparency.** Bankia adheres to a transparent policy on tax management and the payment of its taxes, thus complying with regulatory requirements regarding access to the activity of credit institutions and prudential supervision.
- **Compliance with obligations.** The bank applies at all times the tax regulations applicable in Spain, which is the tax jurisdiction in which all its activity takes place, as well as the pertinent international guidelines and standards, such as the guidelines and action plans of the Organisation for Economic Co-operation and Development (OECD).
- **Risk exposure.** Bankia analyses any transactions involving special tax risk according to their short and long-term impact on the bank's reputation, its shareholders and customers, its relationship with governments and tax authorities and on other areas of the organisation.

The Board of Directors must approve any actions concerning related-party transactions, which are always carried out at arm's length; presence in tax havens (the bank does not operate in them in

order to avoid its tax obligations); the creation of tax structures (which are not used to facilitate tax evasion or to breach the spirit of the regulations); divestitures of companies; the use of tax incentives; relations with the authorities and governments; and the engagement of external tax advisers.

As an expression of Bankia's firm intention to collaborate with public agencies, the bank is an active participant in the Large Businesses Forum, which promotes a more cooperative relationship between Spanish companies and the tax authorities. The Forum advocates a tax policy based on the principles of transparency and mutual trust, through the pooling of knowledge and the sharing of any general problems that may arise in putting the tax system into effect.

The group considers that proper tax management gives it greater legal certainty in tax matters, which benefits its earnings.

In collaborating with the Tax Agency to enhance tax transparency, the bank aims to foster early knowledge of tax policy and facilitate tax risk management. All this will lead to increased legal certainty, lower compliance costs and fewer

disputes with the Tax Agency, besides enhancing the Group's reputation.

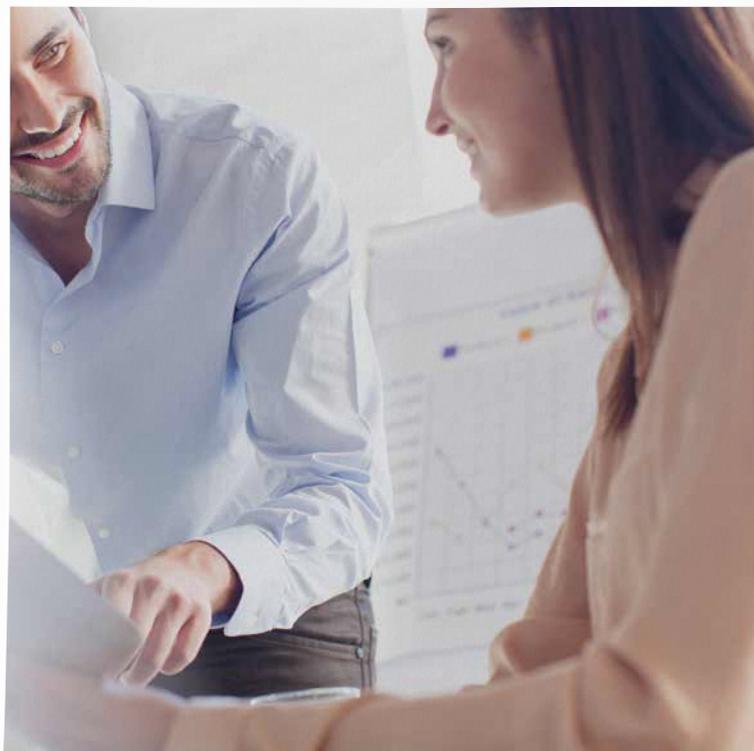
In addition, since 2016 Bankia has been a member of the Tax Agency's Code of Best Tax Practices (CBTP). This code contains recommendations – which are followed voluntarily by the Tax Agency and member companies – aimed at improving the application of the tax system through increased legal certainty, reciprocal cooperation between the Tax Agency and companies based on good faith and legitimate trust, and the application of responsible tax policies in companies, with the knowledge of the Board of Directors.

In 2017, Bankia, as a CBTP member company, drew up its first Annual Tax Transparency Report, with information for financial year 2016, which it plans to submit to the Tax Agency in 2018. This report includes information on certain aspects of the bank's economic activity and funding structure, an explanation of the most significant corporate transactions, details of the group tax strategy approved by the governing bodies and a list of transactions referred to the Board of Directors. It also establishes the extent to which the bank's tax policy is consistent with the principles of the OECD's BEPS (Base Erosion Profit Shifting) package, which is intended to fight tax fraud, erosion of tax bases and the shifting of profits to low-tax jurisdictions.

Additionally, it has taken part in the project to analyse the sector's Total Tax Contribution, carried out by the Spanish Confederation of Savings Banks (CECA), which includes 11 banking groups that together account for 38% of the Spanish financial system. The aim is to analyse the contribution made by the companies that comprise

these groups. The results show that, in 2016, CECA's Total Tax Contribution in Spain was 4,866 million euros. The purpose of this study is to provide reliable data, compiled using a credible and easily understandable methodology, to measure the contribution made by the members of CECA to the Spanish public finances through taxes, for comparison with other similar studies.

On 1 July 2017, the regulations concerning the Immediate Supply of Information on VAT (Sistema de Suministro Inmediato de Información, or SII), came into force. The SII modernises VAT management and improves and promotes the use of electronic media for VAT. The new standard entails keeping VAT records via the Spanish Tax Agency's online office through the almost immediate, daily supply of sales records. Since the new system was introduced, Bankia has complied with the obligations it entails.



### *IN 2017 BANKIA PREPARED ITS ANNUAL TAX TRANSPARENCY REPORT.*

# 03.5

## INTERNAL CONTROL AND COMPLIANCE

### DATA SECURITY

In 2017 Bankia continued to develop the 2016-2018 Strategic Security Plan. The main actions taken were as follows:

- **Security governance.** The Cyber Security Committee, which in 2017 held 12 meetings, gained in importance, as it became one of

the bank's executive committees. Also, a comprehensive awareness-building plan for the period 2017-2018 was put into effect, aimed at making employees and customers more aware of the importance of the individual in maintaining security. A proposal to purchase insurance to cover security incidents was approved.

- **Protection.** New tools were implemented to improve and

extend the scope of supervision and control of vulnerabilities.

- **Surveillance.** A management unit was created to carry out a continuous security assessment and strategies were defined for the use and analysis of Big Data, as part of the trend in security and fraud monitoring towards the implementation of advanced predictive models.

Last year the group also started to use security innovations such as artificial intelligence for mass analysis of network flows and the discovery of suspicious behaviour patterns and Big Data techniques that make it possible to predict attacks.

In 2018 a new Strategic Plan will be drawn up for the period 2019-2021 and work will start on various projects, including the approval and rollout of the Objective Data Security Model, with extended analysis of new risk scenarios and the design of response plans to cyber-attacks and situations of non-availability. Additionally, advanced tools will be implemented to reinforce the existing defences and security in application-managed access by users with privileges.

Biometric data will become particularly important for employee access and access to



resources external to the bank's information systems, in order to raise the level of data protection.

Various context-based factors will be taken into consideration in granting access to information, using what is known as adaptive authentication.

This will help overcome the possible weaknesses of using a password as the sole authentication factor by replacing or supplementing it with other factors.

12

*NUMBER OF MEETINGS OF THE CYBER SECURITY COMMITTEE.*

## **INFORMATION SECURITY, A STRATEGIC FACTOR**

Information is the main asset of any company nowadays and is even more valuable in the digital society in which the bank operates. Information is therefore a strategic asset and so information security is considered strategic in order for the bank to operate and serve its customers.

Bankia defines its information security strategy by adopting a benchmark model based on the most widely recognised information processing and security standards in order to safeguard and protect its customers' information and ensure data integrity, confidentiality and availability whenever customers wish to have access to their information by any means the bank may place at their disposal.

This benchmark model is based on the four main domains on which information security is based: governance, integrated with IT governance and the bank's corporate governance; information protection; surveillance to detect any event that might put information security at risk; and resilience, or appropriate response capacity, to such events.

Every three years, with the assistance of the market's leading consultants and providers, Bankia prepares and executes strategic information security plans in order to be always up-to-date in the face of constantly evolving technology. This enables it to keep up to date with the media through which information is provided to customers, protecting that information, wherever it happens to be, against the ever-present cyber security threats.

In March 2017, Bankia received the CISO Award in recognition of its cyber security policies.