7.

Corporate integrity and ethics

Non-Financial Statement
2023

We are committed to developing and spreading the business values and culture, both internally and externally, and pursuing the fight against corruption with integrity.

7.1 Corporate integrity and anti-corruption

[GRI 2-23]
[GRI 3-3]

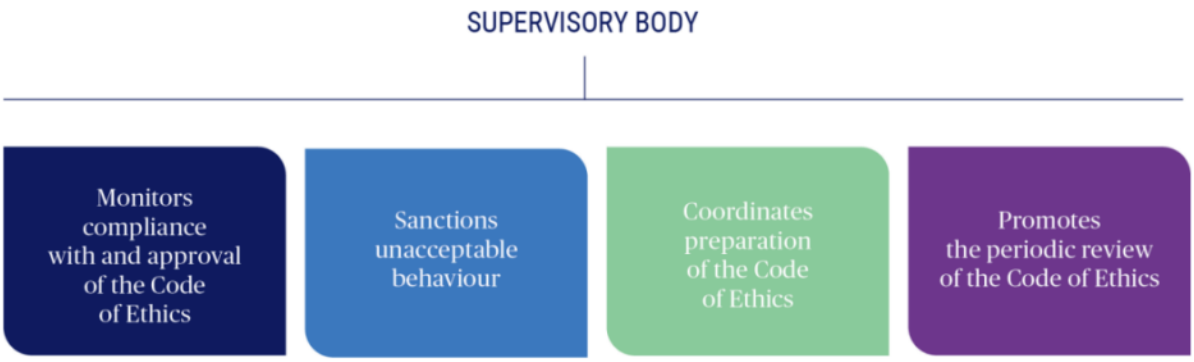
Policies and other reference documentation

- Group Code of Ethics
- Organisational, Management and Control Model as per Italian Legislative Decree No. 231/2001[54]
- Group Whistleblowing Policy
- Group Anti-Money Laundering Policy
- Group guidelines on the Internal Control System
- Internal Control System Policy (Ifis Finance I.F.N. S.A.)
- Anti-Money Laundering Manual Cap.Ital.Fin.
- Banca Credifarma Anti-Money Laundering Manual regulatory/procedural part
- Operating manual on Embargo and anti-terrorism: Checks on incoming and outgoing bank transfers (Banca Ifis)
- Anti-Money Laundering Negative List Operating Manual
- Distribution Policy (Cap.Ital.Fin.)
- Group Lending Policy
- ESG Policy

The Group Code of Ethics, an integral part of the Organisational and Management Model envisaged by Italian Legislative Decree No. 231/2001, outlines the set of principles, values, rights, duties and responsibilities assumed and adopted towards all the stakeholders of Banca Ifis Group, and represents the **"manifesto" of the corporate culture** of Banca Ifis and the other companies of the Group. Making sure that the Organisational Model and the Code of Ethics are effective requires promoting a "culture of control" among all employees and raising the awareness of all structures concerned. This is why the Group trains employees on the contents of the Organisational Model pursuant to Italian Legislative Decree No. 231/01 and the Code of Ethics. Violation of the Code of Ethics by the recipients constitutes a breach of the contractual relationship between Banca Ifis and/or its Subsidiaries and the recipient, and may give Banca Ifis and/or its Subsidiaries the right to terminate or withdraw from the contract for just cause.

As far as the Code of Ethics is concerned, the **Supervisory Body** is responsible for, among other things, **monitoring compliance with it and its implementation**, taking disciplinary action if required, coordinating the drafting of rules and procedures to implement it, promoting a regular review of the Code and its implementation mechanisms, and reporting to the Board of Directors on the work carried out and the problems concerning the implementation of the Code of Ethics.

[54] Adopted by all Banca Ifis Group companies that have appointed a Supervisory Body.



The Code of Ethics clarifies that **the assumption of commitments with the Public Administration and public institutions** is reserved for the appointed and authorised organisational units of the Group, which are required to perform their duties with integrity, independence and fairness. It is prohibited to promise or offer government officials or employees of the public administration in general or of public institutions (including the Supervisory Authorities) payments or benefits to promote or advance the interests of the Group when finalising agreements and supplying services, for the purposes of the award or management of authorisations, when collecting receivables - including due from tax authorities - during inspections or audits, or as part of judicial proceedings.

Anyone either asked for or offered benefits by government officials shall immediately consult with their supervisor and the Supervisory Body, which will assess the adoption of any other initiatives.

Anti-corruption

In order to prevent the risk of committing corruption and bribery, the Group companies that have appointed a Supervisory Body have adopted the Organisational, Management and Control Model as per Italian Legislative Decree No. 231/2001 (OMM), as well as the guidelines set out in the Group Code of Ethics.

In the course of 2023, the Parent Company's Organisation, Management and Control Model was updated in order to adapt the General and Special Parts to the external regulatory changes that occurred in the course of 2023, namely Legislative Decree 24/2023 transposing EU Directive 1937/2019, containing provisions on whistleblowing and the internal regulations newly issued or subject to updates. This regulatory update has also been incorporated into the Organisation, Management and Control Models of the subsidiaries.

The Organisational, Management and Control Models are updated in accordance with the provisions of internal regulations which govern the roles and responsibilities for updating the Models. Specifically, the Group has an operating note governing how to update the model depending on whether it is affected by external or internal regulatory changes or violations.

The Organisational, Management and Control Model as per Italian Legislative Decree No. 231/2001 of the Parent Company covers the following **corruption-related offences**:

- Bribery of office;
- Corruption for an act contrary to official duties;
- Corruption in judicial proceedings;
- Corruption of the person in charge of a public service;
- Bribery, undue inducement to give or promise money or other advantages and corruption;
- Corruption between private individuals;
- Solicitation to commit corruption between private individuals;
- Embezzlement, embezzlement by means of profiting from a third party error;
- Trafficking of unlawful influences;
- Abuse of office.

The Organisational, Management and Control Model as per Italian Legislative Decree No. 231/2001 of the Parent Company specifies that the **structures responsible for monitoring** the commission of potential corruption-related offences are the second and third line of defence functions, the **Supervisory Body, and the Board of Statutory Auditors**.

[GRI 2-24]
[GRI 205-2]

The Board of Directors is briefed on the anti-corruption procedures adopted when it approves the Group's Code of Ethics and Organisation, Management and Control Model[55]. **All employees are required to know and comply with anti-corruption rules**, including with reference to the table attached to the Model that specifically governs potential sensitive activities as well as the main structures and safeguards put into place in terms of policies, internal rules, and control structures. In addition, all the Group's employees can access internal regulations, and specifically the Group Code of Ethics, the Organisational, Management and Control Model pursuant to Italian Legislative Decree No. 231/2001 and applicable protocols and procedures.

The Group makes sure that all employees of the Italian offices receive suitable cyclical training, and whenever the legislation is updated, on the anti-corruption policies and procedures as per the Organisation, Management and Control Model pursuant to Italian Legislative Decree No. 231/01. Specifically, in December 2023, a new compulsory training e-learning course "**The Banca Ifis Code of Ethics**" was published on the Ifis Talent portal, detailing the principles of conduct in relations with employees, collaborators and other stakeholders, as well as the tools for implementing and monitoring the code of ethics. The course includes a final test. Also available is the compulsory training course on Prevention and management of the risk of offences (Italian Legislative Decree No. 231/2001).

The table below provides details of the number of employees who have completed at least one anti-corruption course. **Training on anti-corruption topics** relates only to staff on Italian soil and not to staff in foreign offices.

Number and percentage of employees who received training on the fight against corruption, divided up by category		2023[56]	2022	2021
	No.	**824[57]**	**1557**	**543**
	%	**43%**	**83%**	**29,4%**
Senior managers	No.	29	49	14
	%	26,6%	51,6%	15,7%
Middle managers	No.	224	465	131
	%	37,2%	82,0%	24,0%
Clerical staff	No.	571	1.043	398
	%	46,7%	86,1%	32,8%

In July 2023, the **members of the Parent Company's Board of Directors** approved the update to the Organisation, Management and Control Model pursuant to Italian Legislative Decree No. 231/2001 of Banca Ifis, which also contains rules on the prevention of the risk of the commitment of crimes of corruption and official misconduct.

[55] To date, the Banca Ifis Group has not provided specific training modules on corruption-related offences reserved for Directors. The members of the BoD are made aware of the measures implemented on the matter when approving the Organisation, Management and Control Model pursuant to Italian Legislative Decree no. 231/01 and the Code of Ethics

[56] The count considers employees who have completed at least one of these activities: E-learning course "Prevention and governance of the risk of crime (Legislative Decree. 231/2001)", e-learning course "The Code of Ethics of Banca Ifis", training courses conducted by the Compliance function for colleagues hired with an apprenticeship contract ("Apprenticeship II Year - Compliance") and for colleagues in specific functions ("Prevention and governance of the risk of offences under Legislative Decree 231/2001 and whistleblowing").

[57] The figure refers to Group employees on the workforce at 31/12/2023. Including in the calculation also those employees who left the organisation during the reporting period and who received the training in question during the year 2023 (29, of whom 27 were clerical staff and 2 middle managers), the figures are: total 853 (44,3%); clerical staff 598 (48,9%); middle managers 226 (37,5%); the figures for Senior Managers remain unchanged.

Among the safeguards adopted to **ensure the integrity of the conduct of external networks** is the obligation to comply with the Code of Ethics and the Organisation and Management Model pursuant to Italian Legislative Decree No. 231/01, at the time of stipulating the contract. Finally, as regards the Group's stakeholders, the Group Code of Ethics and the "General Part" of the Organisation, Management and Control Model pursuant to Italian Legislative Decree No. 231/01 are published on the Group's website[58].

[GRI 205-3]

As in the previous year, during 2023 **there were no incidents of corruption or legal cases brought against the employees of the Group or the external networks.**

[GRI 206-1]

As a confirmation of an effective management system, in the course of 2023, in line with previous years, the Banca Ifis Group was **not subject to legal action** for **anti-competitive behaviour, the violation of antitrust regulations and the relative monopolistic practices in which the Group has been identified as a participant**.

Anti-money laundering and terrorist financing

Preventing the risk of money laundering is **key for protecting financial strength** and, more generally, its reputation, and reflects the Bank's and Group's constant effort to actively co-operate with Supervisory Authorities. The Group refuses to do business, either directly or indirectly, with individuals or companies that are sanctioned or are known or suspected members of organisations engaging in criminal or illicit activities. In such situations, Group companies also actively cooperate with the supervisory authorities by initiating, without delay, the activities related to the suspicious transaction reporting process. This principle is translated into **specific procedures and checks** in the various business areas, which aim to assign a risk profile to the counterparty on the basis of which an approval process is activated at different levels of the corporate hierarchy. In the event that a high risk profile is determined, an enhanced review and authorisation of the senior management[59] is carried out.

Specifically:

- the **Leasing** segment examines lists and negative press reports using an automated system integrated with the auto-decision making procedure: if there are any matches, the position is put on hold and marked for a manual assessment, also involving the Anti-Money Laundering function;
- as for the **Trade Receivables** and account products, the above checks are integrated with master data management procedures. Again, depending on the findings, a specific level of money laundering risk is assigned to the counterparty and the decision whether or not to proceed with the opening/prosecution of the relationship is left to the appropriate hierarchical level;
- at **Cap.Ital.Fin.**, screening is carried out to identify politically exposed persons or those at risk of terrorism. The company also has lists in use for screening negative reputational information, which is evaluated on a case-by-case basis on positive subjects, and tools for verifying identification documents;
- at **Banca Credifarma**, possible politically exposed persons or those at risk of terrorism are verified using the Fastcheck procedure, which is integrated into customer profiling applications;
- the **Npl** segment conducts a review at the time the receivables portfolio is acquired as well as subsequent checks on individual counterparties when defining repayment plans and settlement agreements.

[58] For further details, see chapter 7.5 Relationship with the supply chain.

[59] A "Senior Manager" refers to a figure introduced by the anti-money laundering legislation and identifiable in a director, general manager, or other employee delegated by the body with management functions or by the general manager, to follow relations with high-risk customers. This figure has an appropriate knowledge of the level of risk of money laundering or terrorist financing to which the recipient is exposed and is endowed with a sufficient level of autonomy to take decisions capable of affecting that level of risk.

If a relationship with a customer classified as high risk is activated, the position is subject to stricter and more frequent reviews in terms of updates and monitoring operations, and escalation to the Senior Manager for a decision on the maintenance of the current relationship.

Besides being required by law, training is key for raising awareness and promoting a culture among employees of preventing the risk of unwittingly involving the Bank in similar phenomena.

[GRI 2-24]

The Anti-Money Laundering function helps define the contents of **mandatory anti-money laundering training**, especially for those employees that are in direct contact with customers. Training on anti-money laundering is delivered both through classroom courses (in person and/or online) and via the online e-learning course "Anti-money laundering regulations, ed. 2022" lasting 4 hours, activated on the Ifis Talent platform.

More specifically, with regard to classroom training, **a total of 48,5 hours of anti-money laundering training was provided to 552 employees** during the year.

For **Banca Ifis** the following were organised:

- four sessions for the presentation of the AMALTEA SOS tool (the Internal Suspicious Transaction Reporting Form) for First Level Reporting Officers and internal reporting users;
- two sessions of Operating Instructions for the correct identification of the beneficial owner (for Credit Valuation, Leasing Valuation, Corporate Finance);
- a training session to present the AMALTEA MONRAL tool to Unit Managers and Senior Managers;
- additional training sessions are envisaged for the onboarding of new Bank employees.

The following training sessions were organised for **Banca Credifarma**:

- the presentation of the AMALTEA SOS tool (the Internal Suspicious Transaction Reporting Form) for First Level Reporting Officers and internal reporting users;
- the Transaction Monitoring process for Sales Managers;
- screening of negative lists: guidelines and operational aspects for the Operations Unit;
- targeted and specific training for new resource moved within the Operations Unit: list verification, AMLET, transaction monitoring, AUI, payment filtering, SARA flows, SOS;
- operating instructions for the correct identification of the beneficial owner for Sales Managers and Sales Support.

For **Ifis Npl Servicing**, a training session on negative list screening was delivered to the Collections and Payments Unit. In addition, training sessions were held in 2023 to present the AMALTEA SOS (Internal Reporting of Suspicious Transactions) tool to First Level Reporting Officers and internal reporting users for **Capitalfin**, **Ifis NPL Servicing** and **Ifis NPL Investing**. For **Capitalfin** , the virtual classroom training course "Prevention and governance of the risk of crime pursuant to Italian Legislative Decree No. 231/2001 and whistleblowing.

The **Anti-Money Laundering** function participated in training sessions organised by the HR function in connection with the Business Accelerator and Board Member Training programmes of the Parent Company.

Likewise, the Anti-Money Laundering function provided **general anti-money laundering training** to the new Ifis Npl Investing and Capitalfin agents and debt collectors, in addition to specific training sessions of one hour each on "Beneficial owner and the reporting of suspicious transactions" to Ifis Npl Servicing's entire third-party network (financial agents registered with the OAM (Association of Credit Agents and Brokers), debt collection companies, debt collectors pursuant to Art. 115 of the Consolidated Act on Public Safety). The same course will be delivered in January 2024 to the Banca Ifis network (financial agents registered with the OAM who place leasing products) and that of Capitalfin (agents in financial business, registered with the OAM credit mediators).

Whistleblowing

[GRI 2-26]

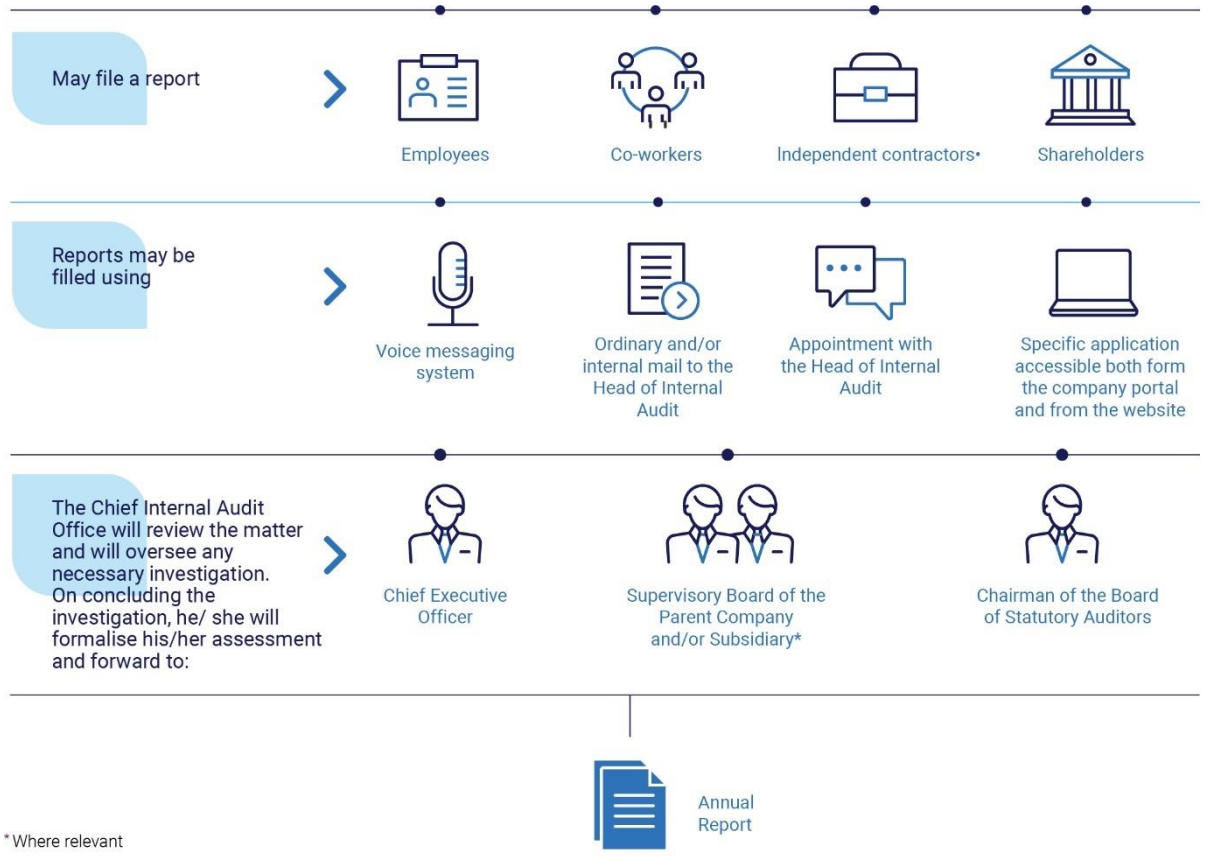
Banca Ifis, as Parent Company, in accordance with regulatory provisions, in particular, most recently, with Italian Legislative Decree 24/2023 implementing EU Directive 1937/2019 on the protection of persons who report breaches of Union law and laying down provisions concerning the protection of persons who report breaches of national laws, and industry best practices, has defined an internal system aimed at enabling the reporting of acts, facts and omissions that may constitute a breach of the laws and internal procedures governing the activities carried out by the Parent Company and its Subsidiaries, while guaranteeing the confidentiality of the personal data of the reporter and the alleged perpetrator of the breach. The whistleblowing system is governed by the Group Whistleblowing Policy, which is part of the Organisational Models of the Banca Ifis Group companies. As detailed in the Whistleblowing Policy, Banca Ifis Group's employees, its collaborators, and licensed independent contractors working with the Group on a regular basis can file a report.

This report may concern any action or omission in breach of the rules governing the Group's operations that causes or could cause harm to Banca Ifis Group. This includes, for instance, actions or omissions, either committed or attempted, which can cause pecuniary damage to the Group, endanger the health or safety of staff or customers or damage the environment, or, as most recently introduced by Italian Legislative Decree No. 24/2023, harm the financial interests of the European Union.

The reports can be submitted using different channels and are handled by the Head of Internal Audit, who examines and investigates them based on the principles of impartiality, privacy, dignity of the employee and protection of personal data.

At the end of the checks, the Head of the Internal Audit function formalises its assessments and forwards them to the CEO (or to the Chairman of the Board of Statutory Auditors in the case of situations of potential incompatibility), and, where relevant, to the Parent Company's Supervisory Body and, in the case of a report concerning an Italian-registered Subsidiary, to the Subsidiary's Supervisory Body, which will assess the necessary corrective actions. The Internal Audit function prepares an annual report on the proper implementation of the process, including aggregate information on the findings of the audits carried out based on the complaints received, that is approved by the Board of Directors and made available to employees.

In 2023, no reports were received through the whistleblowing system.



*Where relevant

7.2 The Internal Control and Risk Management System

[GRI 2-23]
[GRI 3-3]

Policies and other reference documentation

- Code of Ethics
- Organisation, Management and Control Model (pursuant to 231/2001)
- Group ICT and security risk management policy
- Group Credit Risk Management Policy
- Group Operational and Reputational Risk Management Policy
- Group Risk Management Regulation
- Group Market Risk Management Policy
- Group Liquidity Risk Management Policy
- Group Risk Management Policy for Managing interest rate risk on the banking book
- Group Model Risk Management Policy
- Group Anti-Money Laundering Policy
- Group Policy for managing the risk of non-compliance with standards
- Financial Misstatement Risk Management Policy
- Group policy for managing the risk of non-compliance with tax laws
- Risk Management Policy for managing the counterparty, CVA and regulation risk
- Risk Management Policy for managing the Risks of Italian subsidiaries in the banking group
- Group Conflict of Interests Management Policy
- Parent Company Internal Audit Regulation

The Internal Control and Risk Management System

[GRI 2-24]

Banca Ifis Group's internal control system consists of rules, procedures and organisational structures aimed at ensuring, among other things, adherence to the business strategies, the effectiveness and efficiency of processes, and compliance of operations with the law, supervisory regulations, and the policies, procedures and codes of conduct adopted by the Group. All business operations, where envisaged, are subject to audits by the functions or business Areas that own the various processes and operations (line controls or first line of defence), as well as by second line of defence functions (Risk Management, Compliance and Anti-Money Laundering) and third line of defence functions (Internal Audit).

The Risk Management function identifies the risks the Parent and the Group companies are exposed to and measures and monitors them on a regular basis through specific risk indicators, planning potential actions to mitigate material risks[60]. The goal is to provide a unitary and comprehensive view of the risks the Group is exposed to, ensuring an adequate reporting to governance bodies. Risk Management regularly reports to corporate bodies on its operations through the Dashboard - as well as, if required, to the Bank of Italy and Consob (Italy's stock market watchdog).

The Group's overall risk governance and management structure is governed by the Risk Appetite Framework and the relevant documents, which are constantly updated based on the evolution of the Group's strategic framework. Concerning the changes in the Group's scope, Banca Ifis promptly aligns and integrates risk governance and management methods while taking into account the peculiarities of each business.

[60] In response to the 40th update of Bank of Italy Circular 285/2013, the Banca Ifis Group has equipped itself with a second-level control function responsible for the management and supervision of ICT and security risks, assigning the tasks to the Compliance and Risk Management functions, as provided for by the Circular itself.

Specifically, the Group has prepared a Taxonomy of Risks describing how it identifies the existing and/or potential risks the Group could be exposed to in pursuing its strategic goals as well as the tools for preventing and mitigating each type of risk.

The Parent carries out an initial identification of risks based on the list of the minimum risks laid down by supervisory regulations, adding any additional material risks emerged during the analysis of the business model and reference markets in which the Group's companies operate, the strategic outlook, operational methods, and the characteristics of loans and funding sources.

Identifying risks and regularly updating the relevant Taxonomy of Risks is the result of the joint work of second line of defence functions (Risk Management, Compliance, Anti-Money Laundering) and third line of defence functions (Internal Audit), which meet once a year to discuss whether to introduce new risk events and/or review the assessment of potential risks based on the risk management outcomes of the previous year. The Supervisory Body is responsible for identifying and adequately monitoring the existing or potential risks as per Italian Legislative Decree No. 231/2001 relative to actual business processes, constantly updating the mapping of risk areas and "sensitive processes".

The Control and Risks Committee, composed of members of the Board of Directors selected from among non-executive Directors, most of whom are independent, is responsible for supporting the Board of Directors in making investigations, assessments and decisions concerning the internal control and risk management system based on preliminary analyses.

As concerns risk management, the development and dissemination at all levels of an integrated risk culture is fostered in relation to the various types of risk and extended to the entire Group. In particular, training programmes are developed and implemented to make employees aware of their risk responsibilities so that the risk management process is not limited to specialists or control functions. The risk culture is communicated to directors and statutory auditors through special training and induction sessions. Risk induction courses held periodically by the Risk Management function are provided for employees as well.

The audit work performed by the Compliance function (systematic audits and inspections)[61] is based on the plans approved by the Board of Directors and seeks to evaluate the effectiveness of the required, proposed or implemented organisational measures intended to manage the risk of non-compliance. Therefore, these audits apply to all areas for which said risk exists. The audit findings are formally presented in reports shared with the relevant business structures, which must provide feedback on the remedial actions identified and the relevant implementation time line. The function monitors compliance with these requirements and regularly reports to the corporate bodies through the Dashboard - as well as, if required, to the Bank of Italy and Consob.

Concerning the regulations for which there is specialised supervision (e.g.: occupational safety or personal data processing, tax), the responsibilities of the Compliance function can be adjusted, for instance by making the Organisational Unit responsible for coordinating methods, so that it can provide the Corporate Bodies with a comprehensive view of the exposure to the risk of non-compliance. In any case, the Compliance function, at the very least and together with the relevant specialised structures, is responsible for defining non-compliance risk assessment methods, identifying the relevant procedures, and reviewing whether these are adequate.

The Compliance function operates using two types of approaches:

- ex ante: the function provides advice to support the business either as planned, on regulatory topics that are identified and updated under a risk-based approach and in line with the Group's Strategic Plan, or when called upon for specific needs (e.g. new products or operations);

[61] In response to the 40th update of Bank of Italy Circular 285/2013, the Banca Ifis Group has equipped itself with a second-level control function responsible for the management and supervision of ICT and security risks, assigning the tasks to the Compliance and Risk Management functions, as provided for by the Circular itself.

- ex post: the function conducts compliance audits in accordance with the Annual Compliance Plan as well as systematic inspections, whose findings are shared with the functions concerned, reported to the BoD through the Dashboard, and notified to the Bank of ItalyI.

In addition, when starting a major project (such as acquisitions or the launch of new products or operations), the Compliance function actively participates by providing operational and other recommendations on how to properly manage the risk of non-compliance, for instance in terms of precautions and controls to be implemented, regulations to consider, and monitoring actions to be taken.

To promote a culture of respect for the law at all organisational levels, the Group provides refresher courses and training programmes to employees to make sure they acquire and develop the knowledge necessary to comply with the law, internal rules, and industry regulations. Training programmes have also been made available to Group employees throughout FY 2023. The Compliance function informs the structures concerned of any regulatory changes deemed significant in order to initiate the regulatory change monitoring and adoption process, and either provides training or encourages more comprehensive training initiatives by involving the Human Resources function.

The Anti-Money Laundering function performs systematic second line of defence audits concerning the risk of money-laundering and terrorist financing to ensure the relevant procedures are properly applied to operational processes, and develops Key Risk Indicators representing the most significant risk factors to be monitored. It also performs a self-assessment of the risk of money laundering and terrorist financing once a year. The function shares the audit findings and the action plan with the relevant Management. These audits and indicators are also displayed in the Dashboard on a quarterly basis and reported to the Board of Directors as well as, if required, to the Bank of Italy. The Anti-Money Laundering function also monitors the evolution of the relevant legislation, providing the structures impacted with information and taking action for the necessary adjustments including, if necessary, those on processes and internal regulations. In order to guarantee an effective application of anti-money laundering legislation, the function also assures the delivery of training programmes to staff, guaranteeing a complete understanding of the purposes, principles of the obligations and corporate liability in terms of the fight against money laundering.

Internal Audit controls, with a view to assuring level three audits, the regular performance of operations and the evolution of business risks and assesses the completeness, adequacy, function and reliability of the organisational structure and the various components of the Internal Control System. The review carried out by the Internal Audit function is transversal to all corporate processes. In order to identify any abnormal performance or breach of internal regulations and assess the function of the Internal Control System as a whole, the Internal Audit function is specifically assigned responsibility for verifying the correct application of internal provisions. In this specific area, Internal Audit performs annual audits of the risk management activities of the Group's Risk Management function.

The Internal Audit function operates on the schedule approved by the Board of Directors; in addition to this, it also performs unplanned audits as specifically necessary and/or required by the main corporate bodies or external supervisory bodies. The results of the audits are shared with the reference organisational unit and with the level two audit functions and then sent to the Board of Statutory Auditors and the Control and Risks

Committee. The Internal Audit function also reports back regularly to the corporate bodies, also by presenting specific summary reports (Annual reports and Quarterly Dashboards) that, if required, are also submitted to the Bank of Italy or Consob. The audit cycle, as required by the supervisory regulations, is three years and includes audits of all major business processes.

In 2023, the Internal Audit function planned and launched, among others, a verification activity aimed at ensuring the adequacy and compliance with laws and regulations on the protection and management of personal data of the Group's privacy policy, in particular with regard to the Guarantor's Provision No. 2 of 16/6/2004.

The value of ethics: Code of Ethics

[GRI 2-23]

Banca Ifis Group conforms to the purposes and guidelines of the Corporate Governance Code, and its governance system is aligned with the principles contained therein, the relevant recommendations issued by Consob, and, in general, best practices, which are intended to ensure an appropriate separation of responsibilities and powers by striking the right balance between operational and control functions.

Pursuant to Italian Legislative Decree No. 231/2001 on the "Rules for the administrative liability of legal entities, companies and associations, including those without legal status", Banca Ifis Group makes the Code of Ethics and the Supervisory Body's Regulations publicly available.

The Group's Code of Ethics outlines the set of principles, values, rights, duties and responsibilities assumed and adopted in respect of all stakeholders with whom Group companies enter into relations in order to ensure the pursuit of their corporate purpose.

The Code of Ethics provides a set of rules of conduct based on principles of fairness, loyalty and consistency, aimed at continuously reinforcing the ethical-behavioural standards of its recipients and creating a common culture within the Group. Moreover, it represents a constantly updated tool, fundamental to preserve the reputation based on people's trust and reliability, to guarantee a sustainable creation of value over time and, when necessary, to recognise the new principles that the socio-cultural evolution imposes to consider. The values contained therein guide the choices and initiatives adopted by the Group, the definition of internal processes and the conduct of the people who work within it.

The Group Code of Ethics in force today was approved on 22 December 2016 and has been updated constantly, most recently on 13 July 2023. Specifically, the aim of the revision was to update the document in view of the adaptation of internal regulations and reporting channels (whistleblowing) in the face of the transposition, with Italian Legislative Decree 24/2023, of EU Directive 1937/2019 concerning the protection of persons who report breaches of Union law and laying down provisions on the protection of persons who report breaches of national laws. The changes made to the Code of Ethics concern the list of possible internal reporting channels, with the introduction of the voice messaging system, and the description of the new external reporting channels (ANAC and Public Disclosure).

With specific reference to ESG factors, Banca Ifis Group intends to disseminate and consolidate a culture of respect for the environment and social correctness, promoting responsible practices, providing adequate information and training, and requiring employees to report any deficiencies or failures to comply with applicable regulations in a timely manner. Banca Ifis Group has therefore identified the Code of Ethics as a useful tool for the dissemination of these principles, as it asks recipients to consider the environmental and social consequences of all conduct adopted during their work activities, encouraging responsible actions[62].

In accordance with the principles laid down in the Code of Ethics, all Group employees must behave ethically in their relationships with employees and collaborators, customers, debtors, suppliers, the public

[62] When formalising contracts or agreements with suppliers, the Code, according to what is set forth in internal regulations, may be expressly referred to as a binding document, the violation of which will also have contractual consequences.

administration, shareholders and the financial community. Illegal or unethical behaviour, including with reference to legal provisions, codes and regulations adopted by the Group, is not acceptable.

The Organisational and Management Model

[GRI 2-24]

Banca Ifis Group seeks to ensure conditions of transparency and fairness in conducting its business, so as to safeguard its institutional role and image as well as meet the expectations of shareholders and of those who work for and with the Group: to this end, it has decided to adopt the Organisational and Management Model (the "OMG" or "Model") as per Italian Legislative Decree No. 231/2001.

This is a complex set of principles, rules, provisions, and organisational charts with the relevant duties and responsibilities allowing to establish and duly manage a system to control and monitor sensitive operations in order to prevent the risk of committing the offences set out in Italian Legislative Decree No. 231/2001. The Model – adopted in 2004 and constantly aligned with the latest regulatory changes – is part of a broader control system that consists mainly of the Internal Control Systems and Corporate Governance rules of Banca Ifis. The Group's companies adopt the same approach.

In addition, viewing its Model as a key Group policy tool, Banca Ifis extends its internal organisational instruments to its subsidiaries as applicable. To this end, a methodological support function is envisaged, in the General Counsel Department of the Parent Company, for the activities of all the Group's Supervisory Bodies, with the task of drawing up and maintaining, subject to validation by the Compliance function and with the support of any other functions involved, the Supervisory Body Regulations. In addition, it draws up and updates, with the support of the Compliance function, the General Part of the Organisational Models, while with reference to the Special Part of the Organisational Models, it coordinates the Organisation function so that it makes the appropriate updates.

Among other offences, the Model also covers crimes strictly related to non-financial topics, such as corporate offences (corruption and bribery), crimes of manslaughter and negligently causing serious or grievous bodily harm committed with breach of occupational health and safety regulations, as well as environmental offences and crimes associated with human trafficking and exploitation and the employment of illegal immigrants and tax crimes, crimes against cultural heritage and offences concerning means of payment other than cash.

As a result of the update of external whistleblowing regulations in 2023, the Parent Company Model and the Models of the Subsidiaries were revised, most recently in July 2023. In particular, the changes made, as required by the internal decision-making processes, were submitted to the respective Supervisory Bodies and Boards of Directors, for verification and subsequent approval. The review meets the Bank's and Group's need for protection, by incorporating any intervening regulatory and organisational changes, first and foremost through information of the users, namely the Group's employees, managers and collaborators called to ensure that their actions are compliant with the Model and, secondarily, of its potential readers, namely the Investigators called to assess its effectiveness and adequacy.

Monitoring the functioning of, and compliance with, the Organisational Models is the responsibility of the Parent's Supervisory Body and the Supervisory Bodies of the Subsidiaries, if any, which have their own independent powers of initiative and control. Banca Ifis Group's Head of Internal Audit and Head of the Compliance function are members of all Supervisory Bodies and currently play a crucial role in coordinating, integrating and maintaining the information flows required from the Supervisory Bodies of the Group's companies.

Main risks associated with non-financial topics

The Group, over the years and in line with the requirements of Art. 3 of Italian Legislative Decree 254/2016, has activated processes and defined specific responsibilities to identify and manage the main risks relating to ESG topics. The nature of the associated risks and the main risks and how they are currently managed are presented

below for each material topic. The following paragraphs provide specific insights into some of the topics and risks listed in the table below.

For each material topic, Banca Ifis Group has identified the nature of the relevant risks as well as the main risks and how they are currently managed. The findings are summarised in the following table.

Material topics	Nature of risk	Main risks	Main safeguards/mitigating actions
Support to enterprises and financial inclusion	Reputational; Compliance/Operational; Credit	• Failures and mistakes in operations related to financial inclusion initiatives, giving rise to reputational impacts or credit risk	• Credit management policy and subsidised financing procedures • Local information/training initiatives
Diversity, inclusion and employee well-being	Reputational; Compliance/Operational	• Requests for compensation for any form of discrimination based on gender identity, disability, age, religion, nationality, race, personal beliefs, etc. • Reputational and image damage • Harassment and mobbing • Gender pay or wage gap equal employment and skills • Difficulties in access to top positions and/or professional development processes for the less represented gender • Employee workplace injury • Work-related ill health • Injuries attributable to insufficient safety and/or health of work places and tools • Employment instability (e.g. of young employees) due to the use of fixed-term and/or temporary contracts	• Code of Ethics • Whistleblowing • Remuneration and incentive policies • Group employee management policy • Policy to promote diversity and inclusiveness • Gender Equality Management Regulatory Manual • Strategic Plan for Gender Equality • Uni PdR certification: 125 2022 "continuously improving" • Maintenance of WWI (Winning Women Institute) certification • Second level Operational Risk controls on HR litigation • Integrated Safety and Environment Manual • Training on health and safety practices and procedures • Risk assessment document (DVR) • Consolidated Document for the Assessment of Risks of Interference (DUVRI) • Provision in the national collective bargaining agreement determining the limits of employment with fixed-term contracts/administration and significant conversion of fixed-term contracts into open-ended contracts • Second level Operational Risk controls on HR litigation
Promotion and development of employees	Reputational	• Lawsuits against the Group related to the handling of the employment relationship or recruitment, with respect to the course of the working relationship in all of its facets. Examples include, but are not limited to: salary aspects, classification levels, career development, training, etc.	• Group employee management policy • Occupational welfare system • Remuneration and incentive policies • Ifis Academy • Support from external lawyers • Performance appraisal system • Second level Operational Risk controls on HR litigation
Social Banking	Reputational; Compliance/Operational; Credit	• Failures and mistakes in operations related to financial inclusion initiatives, giving rise to reputational impacts or credit risk	• Credit management policy and subsidised financing procedures • Local information/training initiatives
Sustainable business transition	Reputational; Compliance/Operational; Credit	• Failures and mistakes in operations related to financial inclusion initiatives, giving rise to reputational impacts or credit risk	• Credit management policy and subsidised financing procedures • Local information/training initiatives
Digital innovation	Reputational Operational ICT and security	• The risk of loss due to breaches of confidentiality, the lack of integrity of systems and data, the inadequacy or unavailability of systems and data, or the inability	• ICT strategic planning policy • IT Incident Management Procedure • Change Management Policy • Project Management Policy

Material topics	Nature of risk	Main risks	Main safeguards/mitigating actions
		to replace information technology (IT) within reasonable time and cost constraints if the requirements of the external environment or business change (i.e. agility) • Customer dissatisfaction, potentially leading to customer complaints or loss • Malfunctioning or non-operational new technology	• Performance Measurement and Monitoring Policy • Procedure for continuous monitoring of security threats and vulnerabilities • Group ICT and Security Risk Management Policy
Loans and the fight against climate change	Reputational; Credit	• Reputational consequences of negative events concerning the company (operating in sectors with high environmental and/or social impacts) financed by the Group • Insolvency or deteriorating creditworthiness of the counterparties the Group is exposed to	• Leasing: excluded business sectors • Identifying the sectors that pose the greatest reputational risk as part of the policy for Significant Transactions • Sustainability Committee
Direct environmental impacts	Reputational; Compliance/Operational	• Environmental damages caused by failure to comply with environmental management standards or the adoption of inappropriate operations and practices • Negative perception of the Group image and reputation as a result of the above negative events • Climate-related and Environmental Risks • Damage to assets owned by Banca Ifis Group as a result of external events (e.g. earthquakes, landslides, floods) that may cause an interruption of operations • Complaints and disputes • Failure to meet targets in terms of reducing financed emissions	• Integrated Safety and Environment Manual • Group Environmental Policy • The bank incorporates climate-related and environmental risks into its business strategies, governance and RM frameworks in order to mitigate these risks and meet regulatory requirements
Corporate integrity and anti-corruption	Reputational; Compliance/Operational	• Internal fraud, perpetrated by the Group's employees and Agents that work together with the Group • Aggressive debt collection practices and/or instances of abnormal conduct on the part of external collectors and agents • External fraud, traceable to Debt Collection Agencies and/or Financial Agents • Involving, even unwittingly, the Group in money-laundering and terrorist financing	• Code of Ethics • Organisational, Management and Control Model as per Italian Legislative Decree No. 231/2001 • Group Whistleblowing Policy • Specific safeguards for the Group's agents • Systematic anti-money laundering and terrorist financing monitoring • Employee training • Second level Operational Risk controls on anomalous business practices by External Collection Networks
Data protection	Reputational; Compliance/ICT and Security Operations	• Loss or misuse of the Group's data deriving from internal or external threats involving employees or IT systems • Cyber attacks through phishing campaigns	• Centralised organisational structure to manage the Group's Privacy and Security • Technical and organisational measures for information security • Technical and organisational measures to ensure business continuity • Procedures for dealing with computer and IT incidents • Procedures for dealing with IT and security incidents • Group ICT and Security Risk Management Policy • Phishing simulation campaigns

Material topics	Nature of risk	Main risks	Main safeguards/mitigating actions
			• Training plans aimed at consolidating adequate awareness and a corporate culture based on IT security
Transparency	Reputational; Compliance	• Rising customer dissatisfaction, leading to negative turnover • Lower perceived reliability and security of the Bank and the services it provides • Operational risks and ensuing reputational impacts in terms of transparency, eligibility, disclosure, and fiduciary relationship with customers	• Process for approving new products and services, starting new operations, and entering new markets • Products committee • Constant efforts to make operational processes more efficient in order to reduce customer service response times • Centralised organisational structure to manage communications with customers • Grievance mechanisms • Organisational Procedure for the Transparency of Banking and Financial Operations and Services
Supply chain	Reputational; Compliance/Operational; Legal; ESG; concentration; subcontracting	• Reduction in the quality or interruption of services rendered • Violation of mandatory regulations and ensuing sanctions • Loss of market share • Reputational risks deriving from the above events (e.g. sanctions made public, inability to offer contracted services) • Economic losses (or the need to set aside sums of money) linked to disputes of various kinds (e.g. disputes with customers/suppliers)	• Definition of a company sourcing strategy • Analysis of supplier administrative, organisational, capital and reputational aspects • Analysis of ICT and data security aspects • Definition of appropriate contractual standards in order to mitigate identified risks (e.g. prohibitions against subcontracting in certain conditions) • Ongoing analysis of the service levels provided by the supplier, in the light of what is guaranteed in the contract • Definition of an exit strategy if it becomes necessary to suspend the relationship with the supplier • Second level Operational Risk controls on outsourced functions, ICT third parties, suppliers with contracts exceeding 500K • Policy for the outsourcing of business functions; • Group Expenditure Cycle Management Policy

7.3 Data protection

[GRI 2-23]
[GRI 3-3]

Policies and other reference documentation

- Group IT security management policy
- Group ICT and security risk management policy
- IT Incident Management Organisational Procedure
- Organisational Procedure Information security incidents management
- Organisational Procedure Handling of privacy issues concerning the rights of data subjects and the relationship with the Italian Data Protection Authority (Banca Ifis Group)
- Organisational Procedure Management of Personal Data Processors
- Methodological manual for data processing risk analysis and data protection impact assessment (DPIA)
- Privacy regulatory manual
- Group Regulations governing the use of company equipment
- Organisational Procedure for the Operational Management of Systems and Control of Critical Operations
- Group business continuity policy
- Group ICT strategic planning policy (Banca Ifis Group)
- Group Policy for the monitoring and measurement of performance (Banca Ifis Group)
- Organisational Procedure for managing logical access
- Organisational Procedure for the management of the Physical Security of information resources
- Group policy for the management and security of payment services (Banca Ifis, Banca Credifarma)
- Organisational Procedure for the monitoring of security threats and vulnerabilities
- Organisational Procedure for managing information security logs
- Electronic Device Disposal Operating Procedure (Banca Ifis Group)
- Organisational Procedure for Hardening and Patch Management (Banca Ifis Group)
- Information classification and management policy (Banca Ifis Group)
- ESG Policy

The growing spread of ICT products and services based on processing personal data has made **privacy and information security more and more strategic** for companies over the years.

Banca Ifis Group considers the protection of personal data a mandatory principle that is key for building trust and developing a sense of security with customers as well as protecting the Group's reputation. The Group is also committed to **preventing and managing information security incidents in a timely manner in order to protect the Group's proprietary information**, which includes, among other things, the data of customers, employees, suppliers, and any other party with which the Group does business. In the course of 2023, Banca Ifis Group conducted a wide-ranging and in-depth **review of all internal regulations** on personal data protection and set up an **IT tool** for the automated management of the main privacy requirements.

Information security

The **Privacy & Security** Organisational Unit constantly monitors information security and helps assessing IT risk through the Information Security Governance Organisational Unit.

The **information security incident management process** is aimed at ensuring that any unusual events with potential repercussions on the Group's level of physical and logical security and the availability of IT Services are promptly recognised as information security incidents, and therefore addressed appropriately by the competent structures.

The warnings and events that can give rise to security incidents can originate from **various internal channels** (other organisational units) **and external ones** (customers, suppliers, and institutional channels). The Information Security Governance Organisational Unit manages such warnings in partnership with any other concerned and interested parties, based on the extent and type of the event.

Personal data protection

The main internal document governing personal data protection is represented by the **Privacy Regulatory Manual** approved by the Board of Directors of Banca Ifis as Parent Company, and incorporated by the Subsidiaries through a Directive. The Manual and the privacy regulations and procedures make up the privacy management model as well as the set of guidelines and rules defining how personal data is protected within the organisation.

The **Privacy & Security** function, specifically through the Unit dedicated to Privacy:

- **prepares and updates the internal documents** required by privacy regulations;
- **monitors** and regularly **assesses** compliance with regulations and the implementation of the security measures required by law;
- **analyses the personal data processing methods** adopted by the Bank and the relevant risks;
- **assesses the privacy impacts** that result from launching new products and services, starting new operations, entering new markets, and in all instances in which the Bank plans to internally develop or purchase new software;
- **notifies the Bank's organisational units** of any changes in privacy regulations concerning their respective areas of expertise and provides compliance support;
- **supports the Human Resources function** in the development of an adequate company culture in the privacy field and carries out periodic training sessions for staff (employees and non-employees).

In addition, as far as business continuity is concerned, it carries out an impact analysis on business processes and prepares the relevant plan through the **Business Continuity** Organisational Unit.

[GRI 418-1]

In 2023, at Group level, **two complaints** were filed with the Italian Data Protection Authority by customers, relating to alleged privacy violations: in both cases, in light of the defences provided in the responses, the Authority concluded the investigations by ordering the complaints to be filed.

Substantiated complaints concerning breaches of customer privacy and losses of customer data		2023	2022	2021
Total number of complaints documented as received concerning customer privacy breaches	No.	2	4	4
from third parties and substantiated by the organisation	No.	2	4	4
from regulatory bodies	No.	0	0	0
Total number of events relating to substantiated losses and thefts of customer data	No.	47[63]	57	46

The incidents that involved the loss, access or unauthorised disclosure of personal data in 2023 are primarily related to loss or theft of business devices, misdirected documentation via regular mail or e-mail, and lost or stolen paper documentation. **No incident resulted in any communication to the Data Protection Authority or the data subjects**.

[63] The figure represents the total number of incidents that occurred in 2023 involving the loss, access, or unauthorised disclosure of personal data. The events can be divided up between the Group companies as follows: 14 incidents for Banca Ifis, 21 incidents for Ifis Npl Servicing, 8 incidents for Ifis Npl Investing, 2 incidents for Cap.Ital.Fin., 2 incidents for Banca Credifarma.

In order to mitigate exposure to these risks, in 2023 Banca Ifis Group launched internal awareness-raising campaigns on cybersecurity to develop a greater focus on identifying and reporting incidents involving personal data.

Raising employee awareness and the cybersecurity programme

During 2023, Banca Ifis Group ran several **cybersecurity** awareness campaigns aimed at all employees.

In continuity with the previous reporting period, some **awareness campaigns** were followed up on with the Group's employees through the organisation of webinars and classroom training sessions, involving authoritative speakers on cybersecurity, as well as the usual monthly newsletter, **"Flash Cyber News"**, to promote knowledge and awareness among employees of the latest cyber threats and cyber crime actions, providing up-to-date information on cyber protection and useful suggestions for countering them.

Cyber Intelligence services were continued, as was OSINT research carried out in support of the structure's activities and awareness throughout the Group. The Group has confirmed its adhesion to the **CERTFin service** so as to receive real time reports of attempted fraud in the banking area. Such reports have been shared with the colleagues of the other Bank structures concerned.

Finally, multiple **phishing attack simulation campaigns** were run in 2023, aimed at raising employee awareness of cybersecurity.

The campaigns in question are part of a broader **programme of initiatives launched by the Bank to increase the level of regulatory compliance and the cyber security posture necessary to achieve its digital evolution goals**.

7.4 Transparency

[GRI 2-23]
[GRI 3-3]

Policies and other reference documentation

- Group Code of Ethics
- Group customer amicable dispute management policy
- Organisational Procedure for Marketing Communications to Customers (Banca Ifis)
- Organisational Procedure for the management of disputes sent to Banca Ifis Group
- Organisational Procedure for the Transparency of Banking and Financial Operations and Services (Banca Ifis)
- Organisational Procedure for the Transparency of Banking and Financial Operations and Services (Cap.Ital.Fin.)
- Organisational Procedure for the Transparency of Banking and Financial Operations and Services (Banca Credifarma)
- Organisational Procedure for the mass management of economic and contractual conditions of products pursuant to Articles 118 and 126-sexies of the Consolidated Law on Finance (Banca Ifis, Banca Credifarma)
- Group Operational and Reputational Risk Management Policy
- ESG Policy

Transparency of information on products and services

Transparency towards customers impacts their trust in the Group, which represents the basis for a healthy and long-lasting relationship and is therefore an asset to protect and develop. This concerns both the various communications issued by the physical network as well as specific contractual aspects within the different business lines.

The Group establishes direct relationships with its customers and operates guided by principles of professionalism, honesty, and transparency, providing detailed information on their mutual obligations and any potential risks inherent in the transactions carried out.

All contractual relationships, communications, and documents are written in a clear and comprehensible manner, ensuring customers fully understand the decisions they make.

The Npl Area has an additional mechanism in place to guarantee the transparency of the agent-customer relationship: at the end of each visit by the agent, the customer can sign a “Meeting report” describing what transpired during the meeting and any agreements made. Also when transmitting information to external parties, through advertising or other channels, the Group makes sure its communications are honest, true, clear, transparent, verifiable, and consistent with business policies and programmes.

The organisational units that report to the Operations area manage transparency processes towards customers and the terms applicable to the products offered by the Group at a centralised level, as well as for operations subject to transparency regulations (e.g. sending recurring documents to customers) and helping the Business Areas prepare customer communications. The Compliance function supervises the implementation of banking transparency regulations and is also involved in preparing communications about significant changes to the terms and conditions applicable to a product or service to ensure they are written clearly.

[GRI 417-2]
[GRI 417-3]

In 2023, no non-conformities were noted in respect of voluntary codes and/or regulations regarding information about products and services, nor indeed in marketing communications.

Grievance and claim mechanisms

The Group adopts several **mechanisms to receive feedback and grievances** from key stakeholders, and especially employees, collaborators and professionals that work with the Group on a regular basis, as well as through **complaints** from customers or debtors. These mechanisms help management identify potential inefficiencies, anomalies or issues concerning business processes. Therefore, along with the controls, they help evaluate the effectiveness of the management approach to the various topics.

Handling of complaints

[GRI 2-25]
[GRI 2-26]

The **complaint represents** not only a useful instrument to improve the quality of products, services and customer relationships, but also a **way to monitor** the conduct of the business functions and internal and external operators acting on behalf of the Group (such as the front offices and members of external networks), and thus keep the mutual trust between the Group and the Customer alive. Complaints can concern the quality of products and services, as well as the respect for the principles of integrity and fairness, compliance with regulations, non-discrimination and activities to support entrepreneurship and financial inclusion.

The **goal of the complaints handling process is to handle in an appropriate and timely manner any grievance received from customers** unsatisfied with the products and services provided or offered, taking corrective and preventive actions to prevent any problem from recurring in the future. These actions can consist in specific initiatives addressing the individual complaint or the activation of general solutions to address the causes underlying the individual complaint or multiple complaints concerning the same area. In this regard, all staff involved in the handling of complaints have received specific directives regarding the advisability of facilitating the search for a personalised solution aimed at the granting of support measures on a voluntary basis by the institution.

In addition, again with a view to helping customers resolve problems linked to access to credit, particular importance is given in the **training process for staff responsible for handling complaints** and in the **complaint management process** to the issue of reporting to credit databases (Central Risk Office and private databases), in relation to which the Complaints Department has developed specialist skills that make it a point of reference, together with the Supervisory Reporting Service, for other corporate functions.

The **complaints handling policy**, applied at the Group level, sets the guidelines for handling the complaints received by the Group's companies in an appropriate and timely manner based on the principle of the fair treatment of customers and in accordance with applicable laws.

A **Parent Company Complaints Department** has been established, which ensures the centralised management of all complaints, including those received by subsidiaries. The office dedicated to handling complaints receives complaints and duly and impartially handles them, informing the business units concerned from time to time. The Complaints Department reports hierarchically to the General Counsel and functionally to Compliance and operates according to the guidelines set by them.

As far as **second-level control activities** are concerned, it is the established practice of the Operational and Reputational Risks unit to carry out periodic monitoring of complaints as concerns the internal control system. The purpose of this monitoring is to verify compliance with the regulatory time-frames for providing a response, their number and the acceptance rate. The results of these checks are summarised in specific management reports addressed to various structures, including the Parent Company's Complaints Department, as well as in the Risk Management Dashboard.

[GRI 2-16]

On a six-monthly basis, the Head of the Complaints Department prepares statistical data on complaints and other types of amicable disputes handled by the Complaints Department and draws up a summary report presenting the situation for the reference six-month period for each individual company. The report also

contains additional activities carried out by the Complaints Department during the reporting period, such as training activities, inspections, and similar.

The data processing shows, amongst other items, for example but not limited to, the following indicators:

- the total number of complaints received;
- the percentage of complaints accepted;
- the average response time;
- the geographical distribution of complaints;
- the distribution of complaints by customer category, by product/service, by reason for the complaint;
- any corrective actions taken at organisational level as a result of complaints received during the period under review.

The Head of the Complaints Department submits the report on complaints received and the processing produced:

- to the CEO (if any) of the Banking Group company;
- to the General Manager (if any) of the company.

Through the Head of Corporate Affairs:

- to the Head of the control function that manages the non-compliance risk;
- to the General Counsel Department Manager;
- to the Head of Communication, Marketing, Public Affairs & Sustainability.

The half-yearly report prepared is subsequently brought to the attention of the respective Board of Directors.

The Head of the Complaints Department also prepares a consolidated half-yearly report at Banca Ifis Group level on the overall situation of complaints received by all Group companies.

Complaints		2022[64]	2021	2020
Total number of complaints	**No.**	8.838	5.985	6.672
Accepted	No.	1717	762	928
	%	19,4%	12,7%	13,9%
Partially accepted	No.	254	267	342
	%	2,9%	4,5%	5,1%
Rejected	No.	6.867	4.956	5.402
	%	77,7%	82,8%	81,0%

[64] The figures for the year 2023 will be consolidated and approved by the Board of Directors in March 2024 and subsequently published on the company website at https://www.bancaifis.it/reclami/resoconto/.

7.5 Relationship with the supply chain

[GRI 2-23]
[GRI 3-3]

Policies and other reference documentation

- Group Expenditure Cycle Management Policy
- Corporate Goods and Services Procurement Management Organisational Procedure
- Group Code of Ethics
- Organisational, Management and Control Model as per Italian Legislative Decree No. 231/2001 (Banca Ifis)
- Organisational, Management and Control Model as per Italian Legislative Decree No. 231/2001 (Ifis Npl Investing)
- Organisational, Management and Control Model as per Italian Legislative Decree No. 231/2001 (Ifis Npl Servicing)
- Organisational, Management and Control Model as per Italian Legislative Decree No. 231/2001 (Cap.Ital.Fin.)
- Organisational, Management and Control Model as per Italian Legislative Decree No. 231/2001 (Ifis Rental Services)
- Organisational, Management and Control Model as per Italian Legislative Decree No. 231/2001 (Banca Credifarma)
- Group policy for the outsourcing of business functions
- Procedure on the management of the outsourcing of business functions
- Organisational Procedure - ICT Vendor Analysis and Monitoring
- ESG Policy

The supply chain

[GRI 2-6]

Banca Ifis Group governs relations with the supply chain through internal procedures and policies like the Group Expenditure Cycle Management Policy and the Corporate Goods and Services Procurement Management Organisational Procedure, both updated in 2023.

When formalising contracts or supply agreements, subject to the exclusions set forth in the Procedure, the Group requires the acknowledgement and acceptance of the principles laid out in the Group's Code of Ethics, understood as a binding document the violation of which entails contractual consequences. During the course of 2021, following the update of the Code of Ethics, a contractual clause was added that expressly refers, according to the indications of reference internal regulations, to the Code as a binding document in respect of each recipient and, in particular, suppliers. Violation of the Code of Ethics by the recipients constitutes, in the cases set forth in internal regulations, a breach of the contractual relationship between the Group and the recipient, and also gives the Group the right to demand termination or withdrawal from the contract for just cause if, in the unquestionable judgement of the Group, the violation committed is such as to undermine the relationship of trust or cause significant harm to the Group. The right of the Parent Company or its Subsidiaries to claim damages remains unaffected. In the various relationships with suppliers, this clause is therefore being introduced into contractual texts wherever possible. In addition, also when formalising contracts or supply agreements, in accordance with the indications of internal regulations, the Group also requires the acknowledgement and acceptance of the Organisation, Management and Control Model pursuant to Italian Legislative Decree No. 231/01.

[GRI 204-1]

In 2023, the Group used **4.568 suppliers** (4.524 in 2022), mainly based in Italy, of which the main categories related to professional and non-professional services: in particular consultancy or legal services, outsourcing, customer information services and services related to software use or assistance.

The total value distributed to suppliers, divided between Italy and abroad, is shown below:

Proportion of spending on suppliers		2023	2022
Total value distributed to suppliers	**Monetary value (mln Euro)**	286,5	273,8
Total value distributed to suppliers - Italy:	Mln €	277,8	268,1
	%	97%	98%
Italy - North-East	Mln €	91,5	96,5
	%	33%	36%
Italy - North-West	Mln €	99,1	96,5
	%	36%	36%
Italy - Centre	Mln €	65,8	50,9
	%	23%	19%
Italy - South and Islands	Mln €	21,3	24,1
	%	8%	9%
Total value distributed to suppliers - Abroad:	Mln €	8,7	5,6
	%	3%	2%

The Group **selects its suppliers** on the basis of competitive procedures, transparent criteria and objective assessments covering parameters such as quality, usefulness, price, integrity, soundness and the ability to guarantee effective ongoing support, as well as compliance with the ethical standards adopted by the Group. Service providers are also selected by assessing their integrity, fairness and loyalty in conducting business, their ability to meet the obligations of the Code of Ethics and confidentiality, taking into account the nature of the service offered, and their sensitivity to social, environmental and corporate responsibility issues.

[GRI 403-7]

In managing its relations with suppliers, in order to **minimise any negative impacts on health and safety** deriving from the interaction of its business with that of external suppliers[65], Banca Ifis Group implements various measures depending on the work/service agreed upon. More specifically, and if held to be necessary, the Group:

- as prescribed by Italian Legislative Decree No. 81/08, defines the best ways by which to manage interferences and drafts specific documents such as the Safety and Coordination Plan (PSC) and the Consolidated Document for the Assessment of Risks of Interference (DUVRI);
- demands that suppliers incorporate the Bank's Safety Policy, declaring that they will adopt and respect it;
- demands that suppliers produce any qualifications necessary to go about their business, self-certifying requirements of professional suitability and sending the client the Consolidated Document Attesting to Compliance with the Payment of Social Security and Welfare Contributions (DURC);
- takes additional protection measures, the costs of which are specified in the individual contracts (Safety Costs);
- verifies the presence of the Name on anti-money laundering lists;
- current Chamber of Commerce registration and certificate;
- requires a self-declaration of not being in the cases set forth in Italian Presidential Decree 445 of 28/12/2000.

[65] This methodology is adopted for all interventions requiring the use of contractors, self-employed workers, services and supplies.

As far as second-level control activities on the supply chain are concerned, the Risk Management function is responsible for the management and supervision of risks related to outsourcing arrangements within the internal control system. In addition, following the periodic review process on outsourced activities, it reports annually on the outcomes to the Strategic Supervision Body. Starting from the year 2022-2023, an additional verification and monitoring activity by the Operational and Reputational Risks Unit was also established, which concerns specific suppliers with individual contracts exceeding a certain materiality threshold. The results of these analyses are shared with the Chief Operating Officer in order to identify any necessary interventions.