

3.

Ifis Integrity



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

Ifis Integrity represents the Group's integrity, our constant commitment to guaranteeing **credit quality** and spreading awareness of the **business values and culture** both within and outside the Group. We promote virtuous behaviour, consistent with the Group's values, such as the **fight against corruption**, the **protection of our customers' privacy** and attention to sustainability.

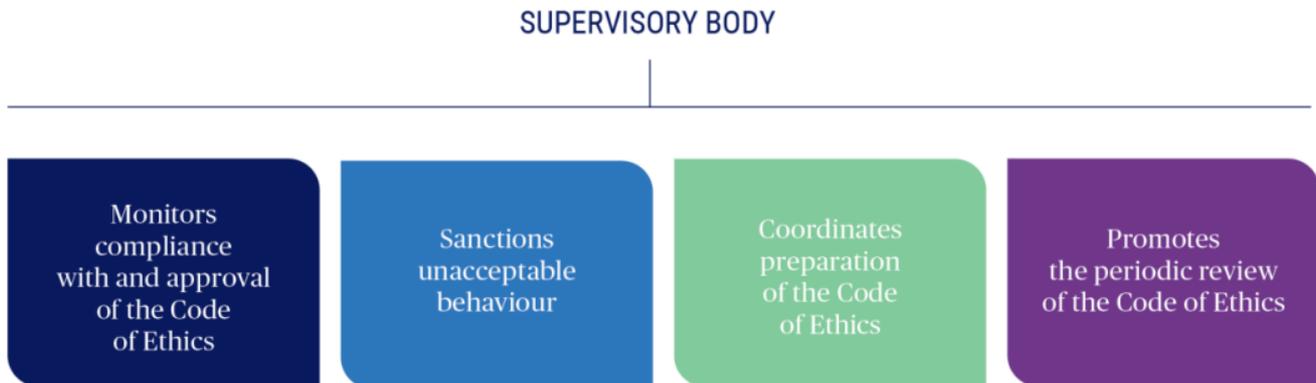
3.1 Corporate integrity and anti-corruption

Policies and other reference documentation

- Code of Ethics
- Organisational, Management and Control Model as per Italian Legislative Decree no. 231/2001
- Group Whistleblowing Policy
- Group Anti-Money Laundering Policy
- Group guidelines on the Internal Control System
- Organisational Procedure Due diligence and customer profiling by risk class - continuously (Banca Ifis)
- Organisational Procedure for Managing tax receivables (Banca Ifis)
- Organisational Procedure for the Management of the Rendimax Current Account (Banca Ifis)
- Organisational Procedure for the Management of the Rendimax Deposit Accounts (Banca Ifis)
- Organisational Procedure for the Management of the Ifis Current Accounts (Banca Ifis)
- Organisational Procedure for Managing tax receivables (Banca Ifis)
- Organisational Procedure for the Management of the Rendimax Current Account (Banca Ifis)
- Organisational Procedure for the Management of the Rendimax Deposit Accounts (Banca Ifis)
- Organisational Procedure for the Management of the Ifis Current Accounts (Banca Ifis)
- Organisational Procedure Management and Concession of Structured Finance
- Organisational Procedure Special Situations Management and Concession
- Organisational Procedure Advisory
- Organisational Procedure Management of distressed loan non-judicial collector network (Ifis Npl Servicing)
- Organisational Procedure Management of distressed loan non-judicial collector network (Ifis Npl Servicing)
- Organisational Procedure Due diligence and NPL customer profiling by risk class (Ifis Npl Investing)
- Organisational Procedure - Collecting captive debts through judicial actions (Ifis Npl Servicing)
- Organisational Procedure Management of acquisitions of credit portfolios (Ifis Npl Investing)
- Organisational Procedure Managing payments associated with captive distressed debt collection operations (Ifis Npl Servicing)
- Organisational Procedure Collecting captive debts through non-judicial actions (Ifis Npl Servicing)
- Organisational Procedure Assigning captive NPLs to debt collection units (Ifis Npl Servicing)
- Organisational Procedure - Due diligence, customer profiling and the reporting of suspicious operations (Ifis Npl Servicing)
- Organisational Procedure for Suspicious Transaction Reports (Banca Ifis)
- Anti-Money Laundering Manual Cap.Ital.Fin.
- Credifarma Anti-Terrorism and Anti-Money Laundering Manual
- Anti-Money Laundering Manual - Farbanca Procedural Part
- Operating manual on Embargo and anti-terrorism: Checks on incoming and outgoing bank transfers (Banca Ifis)
- Operating manual Certification of Positions on Negative Lists
- Distribution Policy (Cap.Ital.Fin)

The **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 the 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 gives 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.



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 has 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 Code of Ethics.

In October 2020, the Parent Company's Organisation, Management and Control Model was updated to assign particular relevance to the reform of the Special Part of the Model and proceed according to the routine directives characterising the document structure, namely: the recording of existing processes and their formalisation, the mapping of inherent risks and the preparation or better presentation of the related measures.

Part of the intervention was aimed at identifying risk areas, in a more detailed, concrete manner than in the previous version of the Model, so as to direct the action of managers, employees and collaborators of the Bank and, consequently, in order to assure an effective Model in accordance with Art. 6 of Italian Legislative Decree no. 231/01.

The offences dedicated greater, priority attention in the context of the update of the Banks' Organisational Model were, for example: money laundering, corporate offences, market abuse and tax crime.

The integrity of the conduct of Group agents

In addition to establishing rules of conduct for its staff, the Banca Ifis Group considers it essential to assure the integrity of conduct of the Leasing area agents too, as well as those of the company Cap.Ital.Fin. and the agents and collection companies of Ifis Npl Investing.

For instance, several precautions are taken to ensure the integrity of the behaviour of debt collection agents and companies, including:

- ensuring observance of the Code of Ethics and Organisational Model envisaged by Decree no. 231/01 when stipulating the contract;
- controlling the number of mandates: agents can have up to three mandates (for financial agents and agents registered with the OAM), and only for non-competing activities;
- adopting an incentive scheme that discourages agents from engaging in inappropriate or persistent behaviour;
- observation of the "Code of Conduct" drafted by the Unirec - Consumer Associations forum.

With reference to the distribution network of Cap.Ital.Fin., the Control Functions carry out regular audits on compliance with reference legislation governing transparency and money laundering. On the basis of the evidence that emerges from the audits performed, specific initiatives are then taken (e.g. training sessions on specific topics), so as to guarantee a high quality standard and professionalism by the distribution network.

As regards the management of the Ifis Npl company call centre Servicing S.p.A., dedicated to phone collection, the organisation of internal work has been optimised and instruments have been created for the constant monitoring and analysis of performance; the aims of these measures include the limitation of the risk of "aggressive" conduct or unfair commercial practices implemented by operators. The company Ifis Npl Servicing S.p.A uses different methods to evaluate the effectiveness of the management approach implemented:

- inquiries by the "monitoring" call centre - separate from the one dedicated to collection operations, which contacts all customers that have successfully repaid their debts thanks to the proposed settlement plans, as well as a sample of customers with whom an agreement has not been finalised, so as to ensure the members of the network acted with fairness and integrity;
- requiring agents to prepare a "Meeting report", when possible, at the end of each visit with a customer describing what transpired during the meeting and any agreements reached. This report must be signed by the customer, so as to keep a transparent and objective record of any agreements reached;
- reviewing any rejected complaints on a quarterly basis to identify potential emerging problems or issues of increasing interest to customers, so as to define the necessary corrective actions;
- constantly monitoring the Company's social channels;
- interviewing customers that have successfully repaid their debts, as per the first point;
- constantly listening to the grievances and needs of network agents with specifically-organised meetings.

The Organisational, Management and Control Model as per Italian Legislative Decree no. 231/2001 of Banca Ifis 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 Banca Ifis 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 205-2]

The Board of Directors is briefed on the anti-corruption procedures at the time it approves the Group's Code of Ethics.¹⁷ 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 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. More specifically, starting July 2020, the new edition has been published on the corporate intranet of the mandatory training course on the "Administrative liability of Entities ed. 2020," also available for 2021. The table below provides details of the number of employees who have completed at least one anti-corruption course. Training on anti-corruption issues 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 | | 2021 ¹⁸ | 2020 | 2019 |
|--|--------------|--------------------|--------------|--------------|
| | No. | 543 | 691 | 476 |
| % | 29,4% | 40,0% | 27,2% | |
| Senior managers | No. | 14 | 14 | 8 |
| | % | 15,7% | 17,9% | 10,8% |
| Middle managers | No. | 131 | 179 | 116 |
| | % | 24,0% | 35,3% | 22,7% |
| Clerical staff | No. | 398 | 498 | 352 |
| | % | 32,8% | 43,6% | 30,1% |

In October 2020, 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, which also contains rules on the prevention of the risk of the commitment of crimes of corruption and concussion, while in August 2021 they approved the updating of the Code of Ethics.

In addition, in 2021 a training course was launched for the top management of the Banca Ifis Group, structured into several meetings in a virtual classroom, which saw the involvement of both expert teachers and professionals of excellence, identified through Abiformazione and the Polytechnic of Milan, and internal managers with the aim of aligning the participants on the Bank's plans and policies. The contents of the plan focused on the elements of strategic and organisational change that the banking sector is facing and on the control of the most important risks; the modules examined in depth the role and responsibilities of the top management Bodies, the market in which the Group operates

¹⁷ 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. Specifically, the update of the Code of Ethics, integrated into the "General Part" of the OMM, was approved in 2021.

¹⁸ The count considers employees who have completed at least one of these activities:

- E-learning course "The liability of entities ed. 2020", made available starting October 2020
- Training courses with external suppliers

and the main challenges that the evolution of the context poses to the banking sector. Specifically, the topics covered in 2021 were:

- Banking sector scenarios also at the international level;
- ESG dimensions between Risks and Opportunities;
- The regulation of related party transactions;
- Fintech and business model innovation;
- Key regulatory changes and the 2021-2022 outlook;
- Strategic risk.

Several precautions are taken to ensure external networks behave with integrity: among other things, it requires them to abide by the Code of Ethics and the Model pursuant to Italian Legislative Decree no. 231/01, at the time of stipulating the contract.

More specifically, following the 2020 update of the Model and Code of Ethics, in January 2021, the new documentation was sent out to the agents and suppliers of Banca Ifis by e-mail. During the course of the year, the further updating of the Code of Ethics included the integration of a contractual clause that will expressly refer 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 a breach of the contractual relationship between Banca Ifis and/or its Subsidiaries and the recipient, and also gives Banca Ifis and/or its Subsidiaries the right to demand termination or withdrawal from the contract for just cause if, in the unquestionable judgement of Banca Ifis and the Companies, the violation committed is such as to undermine the relationship of trust or cause significant prejudice to the Parent Company and/or one of its Subsidiaries. The right of the Parent Company or its Subsidiaries to claim damages remains unaffected. In the various dealings with suppliers (both existing and new) the contractual texts are therefore being adapted, where possible, to comply with these provisions.

Finally, as regards the Bank's stakeholders, the Code of Ethics and the "General Part" of the Organisation and Management Model pursuant to Italian Legislative Decree no. 231/01 are published on the Group's website.

[GRI 205-3]

As in the previous year, during 2021 there were no incidents of corruption or legal cases brought against the employees of the Group or the external networks.

Anti-money laundering and terrorist financing

Preventing the risk of money laundering is **key for protecting the Bank's financial strength** and, more generally, its reputation, and reflects its 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 known or suspected members of organisations engaging in criminal or illicit activities. This principle translates into **specific procedures and audits** in the various business areas:

- the **Leasing** segment examines 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, involving also the Anti-Money Laundering function. Following these checks, the position is assigned a risk profile that serves as the basis for activating an approval process at different hierarchical levels;
- as for the **Trade Receivables** and account products, the above checks are integrated with master data management procedures. Also in this case, based on the matches found, the counterparty is assigned a specific level of money laundering risk, and the decision of whether to open/maintain the relationship is left to the appropriate hierarchical level;
- in **Capitalfin**, screening is carried out to identify politically exposed persons or those at risk of terrorism. In the event of a positivity for politically exposed persons, enhanced verification and authorisation by senior

management¹⁹, and elevation of the risk profile, shall occur. In case of confirmed presence in the terrorist lists, the request is immediately rejected as well as the sending of a suspicious transaction report. The company also has in use lists for screening negative reputational information, which is evaluated on a case-by-case basis on positive subjects, and tools for verifying identity documents;

- in **Credifarma**, possible politically exposed persons or those at risk of terrorism are verified. In the event of a positive finding for politically exposed persons, further investigation is carried out in order to assess the increase in the degree of risk and authorisation of senior management. Lists on negative reputational information are also in use and are subject to constant verification, as are databases for checking identity documents. The company also identifies any changes at corporate level, in particular due to changes in the ownership structure and/or business name and any extraordinary financial transactions carried out;
- list screening for politically exposed persons and terrorists applies in **Farbanca**. Managers carry out in-depth analysis with the customer and evaluate in the Fastcheck procedure, informing the AML function of the results in order to correctly manage the master notes. In the event of positivity on politically exposed persons, the Senior Management authorisation process is activated for the continuation of relations and the raising of the risk profile. These list checks are performed on an ongoing basis;
- the **NPL** segment conducts a review at the time the receivables portfolio is acquired as well as subsequent checks on individual counterparties when defining settlement plans.

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 any decision is escalated 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 this kind of incidents.

Anti-Money Laundering helps define the contents of **mandatory anti-money laundering training**, especially for those employees that are in direct contact with customers. In both 2020 and 2021, training on anti-money laundering was delivered both through (virtual) classroom courses and via the on-line e-learning course "Anti-money laundering regulations, ed. 2020" lasting 4 hours, activated on the Ifis Talent platform. During the year, a total of 2.312,5 anti money laundering training hours were delivered (approximately 4.217 in 2020 and 2.366 in 2019). In particular, the e-learning course was used by 332 Group employees.

- for Banca Ifis, 12 virtual classroom training sessions of two hours each on "Money Laundering Prevention in the Time of the COVID-19 Emergency" were organised for both employees of the Anti-Money Laundering function and employees of the commercial, evaluation and management functions of the bank, for a total of 341 employees. The same class was offered to Business Unit managers and control function staff (47 participants), who were given 3 training sessions of two hours each;
- additional training sessions were organised for the onboarding of 30 new employees including apprentices and new commercial developers and for specific operational topics for 21 employees in the accounts receivable management and payments and payment card departments;
- for Credifarma and Farbanca, a two-hour training session on "Prevention and management of the risks of money laundering and terrorist financing" was organised for 57 employees.

Similarly, the Anti-Money Laundering function provided specific training sessions of one hour each on the subject of "Active Collaboration and Reporting of Suspicious Transactions" to the entire third-party network of the Bank (agents in financial activity registered with the OAM who place the leasing product) and Ifis Npl Servicing (agents in financial activity registered with the OAM, debt collection companies, debt collectors pursuant to art. 115 of the Consolidated Act on Public Safety); and to the new agents and debt collectors of Ifis Npl Investing.

¹⁹ "Senior management" refers to a figure introduced by the AML regulations that can be identified as a director, general manager, or other employee delegated by the governing body or general manager to deal with high-risk clients. This person has appropriate knowledge of the level of money laundering or terrorist financing risk to which the recipient is exposed and has sufficient autonomy to make decisions affecting that level of risk.

Whistleblowing

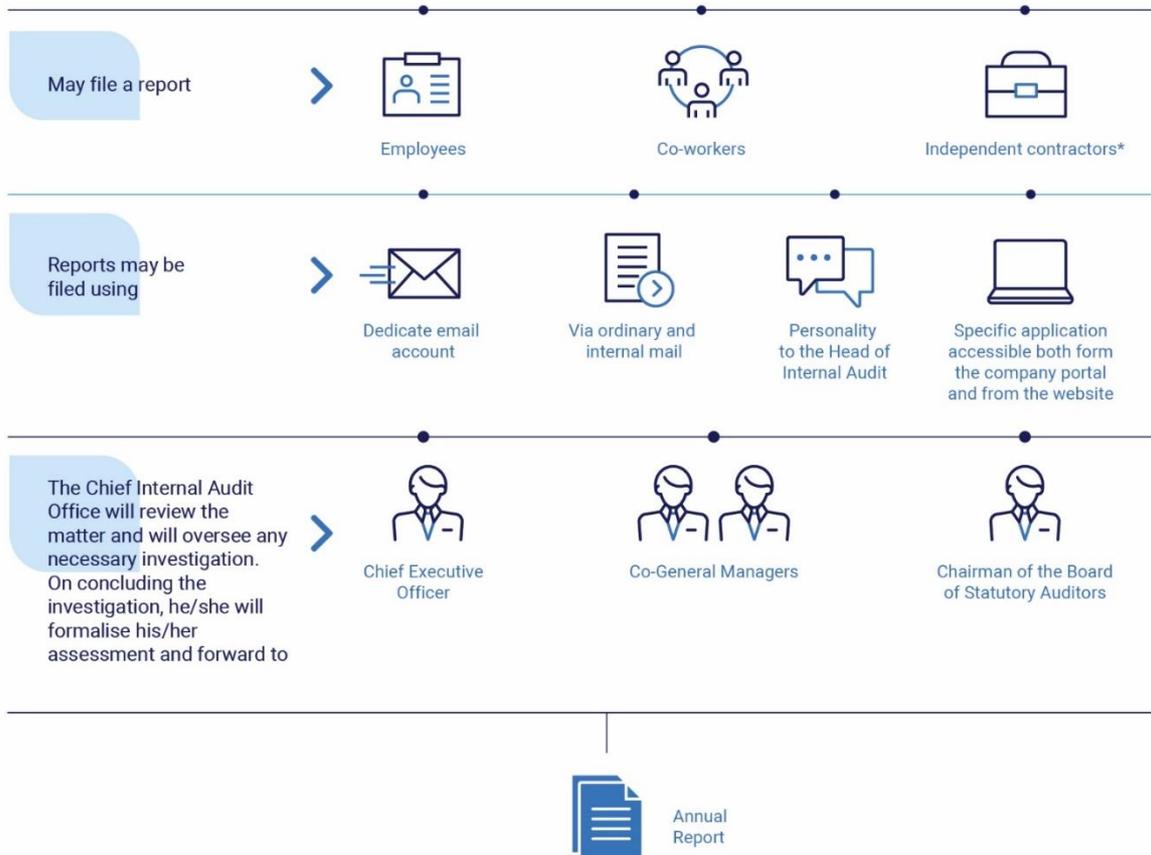
As the Parent company, Banca Ifis, in accordance with industry regulations and best practices, has established an internal system allowing to report actions, events or omissions potentially in violation of laws and internal procedures governing the operations of the Parent and its Subsidiaries with the guarantee that the personal data of the complainant and the alleged offender will remain confidential. **The whistleblowing system is governed by the Group Whistleblowing Policy**, which is part of Banca Ifis's Organisational Model and adopted by the Group companies. The 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 the 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.

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.

After completing the investigation, the Head of Internal Audit formally submits his or her assessment to the Chief Executive Officer (or the Chairman of the Board of Statutory Auditors in the event of potential incompatibilities), who will decide what corrective actions need to be carried out. Internal Audit 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 2021, 2 reports were recorded through the Whistleblowing system.



*Independent contractors who work prevalently and continuously with the Group.

3.2 Credit quality

Policies and other reference documentation

- Group system of delegation of authority to manage credit risk
- Group system of delegated powers on the assumption of credit
- Group system of delegated powers for the assumption and management of the credit risk (Cap.Ital.Fin.)
- System for the delegation of hiring and management powers Ifis Finance IFN SA
- Proxy system for the assumption and management of credit risk IFIS FINANCE
- Group Policy for managing the Most Significant Transactions (MSTs)
- Group policy for reviewing business operations
- Ordinary credit management policy: PHARMA BU (Banca Ifis)
- Ordinary credit management policy: Pharmacies BU (Banca Ifis)
- Ordinary credit management policy: Impresa Italia (Banca Ifis)
- Policy for the management of the collection of distressed captive loans (Ifis Npl Servicing)
- Impairment Policy
- Policy for managing portfolios of receivables purchased outright and due from Public Administration entities (Banca Ifis)
- Ordinary debt collection and monitoring policy (Banca Ifis)
- Monitoring and collection policy (Cap.Ital.Fin.)
- Monitoring and collection policy (Credifarma)
- Policy for the management of the process of verifying the correct monitoring and adequacy of the collection process (Banca Ifis)
- Methodological manual individual evaluation of non-performing loans (Banca Ifis)
- Organisational Procedure Management of tax receivables (Banca Ifis)
- Operating note Leasing preliminary investigation process (Banca Ifis)
- NO 111 - Leasing BU - Redemption assessment and setting process (Banca Ifis)
- NO 103 - Leasing BU - Subjective credit quality assessment (Banca Ifis)
- Leasing debt collection and monitoring policy (Banca Ifis)
- Policy for managing the acquisitions of distressed loan portfolios and relating monitoring (Ifis Npl Investing)
- Distribution Policy (Cap.Ital.Fin.)
- Policy for the management of the collection of distressed captive loans (Ifis Npl Servicing)
- Procedure for Assigning NPLs to debt collection units (Ifis Npl Servicing)
- Organisational Procedure for Collecting debts through judicial actions (Ifis Npl Servicing)
- Organisational Procedure for Collecting debts through non-judicial actions (Ifis Npl Servicing)
- Organisational Procedure for Managing payments associated with distressed debt collection operations (Ifis Npl Servicing)
- Organisational Procedure - Concession and Management of Structured Finance (Banca Ifis)
- Organisational Procedure - Concession and Management of Special Situations (Banca Ifis)
- Organisational Procedure Management of distressed loan non-judicial collector network (Ifis Npl Servicing, Ifis Npl Investing)
- Policy on insurance distribution carried out by the Bank (Banca Ifis)

Credit quality is closely associated with financial strength, which is key for the sustainability of the Group's business model and represents one of the **pillars of the Group strategy**.

In order to incorporate the impacts of the health emergency, analyses were performed, and new prudent logics implemented, as well as the institutional measures introduced to temporarily support the national economy. For more information on the impacts of COVID-19 on the financial position and business performance, please refer to the paragraph entitled "Risks, uncertainties and impacts of the COVID-19 epidemic", Part A - Accounting policies (A.1 - General part, Section 5 - Other aspects) of the "2021 Consolidated financial statements and reports".

The quality of credit can significantly affect the Bank and Group's share price, credit rating, dividends, and financial position - all of which are material to shareholders, financial analysts, ratings agencies, lenders, and Supervisory Authorities - as well as customer trust in the Group's ability to service its obligations, which is especially important for the retail customers of the Rendimax product.

In the case of **Trade Receivables**, the Group's commitment to safeguarding its capital position and credit quality translates into three levels of counterparty checks, so as to prevent the risks of default as well as of involvement in transactions with potentially damaging reputational consequences:

- **automated checks** on both individuals and legal entities to determine whether the prospective customer is on watch lists (terrorism, embargoes, etc.) or lists of "Politically Exposed Persons"; based on the level of risk, Anti-Money Laundering also analyses press reports;
- **individual assessment** by the Transaction Assessment and Counterparty Assessment Teams of the customer, the invoice sellers, and the factored exposure; system of delegation of authority to assume credit risk based on the amounts and risk classes involved;
- **continuous dialogue with the national network**, which may provide reports and feedback on potential clients.

As for **salary- and/or pension-backed loans**, the Banca Ifis Group, in accordance with privacy regulations, considers also the family situation if relevant to assessing the reliability of customers.

The policies governing **Leasing** operations describe how to evaluate the future user of the asset based on reliability and credibility criteria through a scoring system and the preliminary work carried out by specialised teams. Specifically, these assess the soundness of the counterparty's credit position and whether the requested asset is consistent with its operations.

Credit monitoring as well as the monitoring of individual exposures are conducted on a regular basis using effective procedures that can provide timely warnings of potential issues and ensure the adequacy of impairment losses and write-offs. Risk Management ensures the credit monitoring of individual exposures, specifically non-performing ones, is properly carried out and evaluates the consistency of the classifications, the provisions set aside, and the adequacy of the debt collection process at the central and peripheral level.

The Group companies operating in the **NPL** segment, which specialise in acquiring and managing non-performing loans, focus on assessing whether the receivables can be recovered and preparing settlement plans compatible with the specific debt situation by adopting **several mechanisms throughout the various loan acquisition stages**:

- first, it verifies whether the loans being acquired can be recovered, so as to exclude non-existing or time-barred receivables and prevent the risk of non-payment as well as the reputational risk that trying to collect bad loans would entail. After establishing a first contact with the account debtors, the NPL Area assesses the legitimacy of any complaints and, if these are based on reasonable grounds, writes off the position or seeks indemnification from the seller, if allowed by the contract;
- it prepares settlement plans suited to the customer's finances and tailored to each individual case;
- it assesses the probability the customer will actually settle its debts.

Identification of the **Operating Segments** is consistent with the methods adopted by the Management to take operative decisions and is based on internal reporting, used in order to allocate the resources to the various segments and analyse the relevant performance.

In line with the structure used by Management to analyse the Group's results, the information by segment is broken down as follows:

- **Commercial & Corporate Banking Segment**, represents the commercial offer of the Group dedicated to companies and consists of the Business Factoring, Leasing and Corporate Banking & Lending;
- **Npl Segment**, dedicated to non-recourse factoring and managing distressed loans, servicing and managing non-performing, secured loans;
- **Governance & Non-Core Services Segment**, which provides the segments operating in the Group's core businesses with the financial resources and services necessary to perform their respective activities. The Segment includes treasury and proprietary securities desk activities, the disbursement of salary- or pension-backed loans and some portfolios of personal loans, as well as some corporate loans portfolio assigned for run-off insofar as held to be non-strategic to the Group's growth.

During 2020, changes were made to the Operating Segments in order to fully implement the Group's business model. Therefore, the information given in this document is in line with the new Segment reporting.

Below are the values of the Gross and Net NPE ratio of the Commercial & Corporate Banking Segment. The Gross Ratio is in line with 2020, while the Net Ratio has increased since 31 December 2020.

| GROSS AND NET NPE RATIO | | 2021 | 2020 | 2019 |
|-------------------------|---|------|------|------|
| Gross | % | 5,9% | 5,9% | 8,5% |
| Net | % | 3,6% | 2,7% | 4,2% |

In total, the ratios calculated on receivables due from customers, net of the NPL Segment and government securities included in that item, are:

- Gross Ratio: 6,4% (6,4% at 31.12.2020)
- Net Ratio: 3,9% (3,2% at 31.12.2020)

3.3 Data protection

Policies and other reference documentation

- Group IT security management policy
- Group IT risk assessment and management policy
- 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 (Cap.Ital.Fin., Ifis Rental Service, Ifis Npl Servicing, Ifis Npl Investing, Ifis Real Estate, Farbanca, Credifarma)
- 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
- Group business continuity policy
- Group ICT strategic planning policy (Banca Ifis, Farbanca, Ifis Finance)
- Organisational Procedure Management of the development, purchase and maintenance of the application software and technological infrastructure
- Group Policy for the monitoring and measurement of performance (Banca Ifis, Ifis Finance)
- Organisational Procedure for managing logs (Banca Ifis)
- Organisational Procedure for managing logical access (Banca Ifis)
- Group internet payment system policy (Banca Ifis, Ifis Finance)

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.

The 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 Bank's proprietary information**, which includes, among other things, the data of customers, employees, suppliers, and any other party with which Banca Ifis does business. 2020 saw the Group further consolidate the measures required by the European General Data Protection Regulation (GDPR).

Information security

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

Raising employee awareness and the Cybersecurity Programme

In order to raise the awareness of all its colleagues to the topic of cybersecurity, in 2021, the Banca Ifis Group made multiple communications with a view to alerting recipients to the risks of the campaigns in progress. In continuity with the previous reporting period, an awareness campaign was launched among the Group's employees through the initiative "Ifis Talks - Technology through the eyes of a hacker: Cyber Security concerns everyone" to promote knowledge and awareness among employees of the latest cyber threats, providing up-to-date information on cyber protection and providing useful suggestions for countering them. This initiative was implemented on the occasion of the month dedicated to the topic of IT security in which Banca Ifis adheres to the European Union's ECSM (European Cybersecurity Month) campaign.

Cyber Intelligence services were continued, as was OSINT research carried out in support of the structure's activities and awareness throughout the company. The Group has adhered 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.

In addition, stringent protective measures have been taken to further reduce the level of risk in specific areas:

- the bank's e-mail infrastructure, through the introduction of an anti-phishing system to detect malicious e-mails more effectively;
- corporate passwords, through an increased complexity of the same, with the simultaneous gradual introduction of Multi Factor Authentication to the entire corporate population;

Finally, a phishing attack simulation campaign aimed at raising employee awareness of cybersecurity was conducted in 2021.

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

Activities to improve the level of information security include:

- the introduction of network security measures to further protect the bank's technological perimeter;
- the expansion of the scope of security testing, an activity aimed at identifying any vulnerabilities and remedying them;
- the execution of Red Teaming activities, i.e. activities that are characterised by the ability to simulate a real adversary that attempts to violate the technological perimeter of the exposed services, web applications, etc. This allows the company to train the teams in charge of responding to cyber attacks, also identifying possible areas for improvement;
- the simulation of targeted ransomware campaigns in order to raise awareness about the risks associated with this type of threat.

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 internal channels (other organisational units) or 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. Said document and the privacy regulations and procedures make up the privacy management model as well as the set of guidelines and rules defining how 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 Human Resources 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 2021, as for last year, the Group received 4 complaints concerning privacy breaches, almost all associated with operational mistakes/human error. In any case, no sensitive data was exposed.

| Substantiated complaints concerning breaches of customer privacy and losses of customer data | | 2021 | 2020 | 2019 |
|---|-----|------------------|------|------|
| Total number of complaints documented as received concerning customer privacy breaches | No. | 4 | 4 | 4 |
| <i>from third parties and substantiated by the organisation</i> | No. | 4 | 4 | 4 |
| <i>from regulatory bodies</i> | No. | 0 | 0 | 0 |
| Total number of events relating to substantiated losses and thefts of customer data | No. | 49 ²⁰ | 32 | 10 |

The growing number of incidents that entailed the loss, access or unauthorised disclosure of personal data in 2020 is mainly due to an increase in the dangers and risks of cyber attacks in connection with the new methods of remote working. In order to mitigate exposure to these risks, in 2020 the Bank launched an internal awareness-raising campaign on cybersecurity.

As a result of the many awareness and sensitization activities put in place during the year, Banca Ifis employees have developed a greater focus on identifying and reporting incidents involving personal data. For this reason, in 2021 the upward trend in the number of incidents is confirmed, compared with the previous reference period, which did not, however, give rise to any communication to the Data Protection Authority or to the data subjects. As further explanation of the increasing trend, it is noted that verification activities were carried out on certain business processes that allowed for more accurate detection of personal data breaches. Incidents noted in 2021 are primarily related to loss or theft of business devices, misdirected documentation via regular mail or e-mail, and lost or stolen paper documentation.

²⁰ The figure represents the total number of incidents that occurred in 2021 involving the loss, access, or unauthorised disclosure of personal data. The events can be divided up between the Group companies as follows: 19 incidents for Banca Ifis, 24 incidents for Ifis Npl Servicing, 4 incidents for Ifis Npl Investing, 1 incident for Cap.Ital.Fin., 1 incident for Credifarma.

