# Emerging risks


Itaú Uinbanco Holding S.A.

# risk management

Undertaking and managing risks is the essence of our business and a responsibility of all of our employees. We have well-established rules and goals that help us understand, identify, measure, manage, and mitigate risks are key practices to our business.

> **“We are a universal bank, operating predominantly in Latin America. Supported by our risk culture, we operate based on rigorous ethical and regulatory compliance standards, seeking high and growing results, with low volatility, by means of long-lasting relationship with clients, correctly pricing risks, well distributed fund-raising and proper use of capital”.**
>
> Board of Directors Statement

Our risk appetite defines the nature and level of acceptable risks, and our risk culture guides the initiatives that are part of the strategic risk management work and the development of tools that enable implementing the principles of our risk culture:


- Risk management principles:
  - _ Sustainability and client satisfaction;
  - _ Ethics and respect for regulations;
  - _ Risk pricing;
  - _ Diversification;
  - _ Operating excellence; and
  - _ Risk culture

- Follow-up quantitative metrics:
  - _ Capitalization: capital ratios in normal and stress situations; and debt issuance ratings.
  - _ Liquidity: short- and medium-term liquidity indicators.
  - _ Composition of results: largest credit risks; largest exposures and exposures by rating brackets; concentration by industries, countries, and segments; and concentration of market risk.
  - _ Operational risk: operational loss events; and Information technology.
  - _ Reputation: suitability indicators; media exposure; client complaint tracking; and regulatory compliance.

## management model

Our risk management organizational structure complies with Brazilian and applicable international regulations currently in place and is aligned with best market practices.

Our risk management model consists of three lines of defense: the business areas bear primary responsibility for risk management, tracked by the risks area, and, lastly, the audit area subordinated to the Board of Directors:

Capital and Risk Management Committee - Pedro Bodin[1]

Monthly Risk Appetite Monitoring

Board of Directors
Pedro Moreira Salles
Roberto Egydio Setubal

Audit Committee
Gustavo Loyola

Discussion of metrics and the outcome of Risk Appetite, as well as the main risk topics

Internal Audit
Paulo Miron

3rd line of defense

**Independent review** of the activities in which the institution is engaged

Itaú Unibanco Holding
Milton Maluhy

André Rodrigues
Retail banking, digital channels, UX, insurance and SME finance

Carlos Constantini
Wealth Management & Services (WMS)

Pedro Lorenzini
Treasury, asset products and client desks, macroeconomics and operations in South America

Alexandre Zancani
Auto loans, mortgages, "consórcios", credit for individuals and recovery, among other

Flavio Souza (Itaú BBA CEO)
Commercial bank, CIB, ECM and DCM, research and wholesale credit

André Sapoznik
Payments, operations, services and marketing

1st line of defense

**Manages the risks these generate,** with responsibility for identifying, assessing, controlling and reporting

Alexsandro Broedel (CFO)
Finance and investor relations, real estate assets and procurement

Matias Granata (CRO)
Market, credit and operational risks, capital management, corporate security, compliance and AML

2nd line of defense

**Ensures that the risks are managed and based on the principles of risk management:**
-risk appetite;
-policies;
-procedures; and
-dissemination of the risk culture in the business

Sergio Fajerman
Human Resources

Leila Melo
Legal, ombudsman, institutional communications, sustainability and government relations

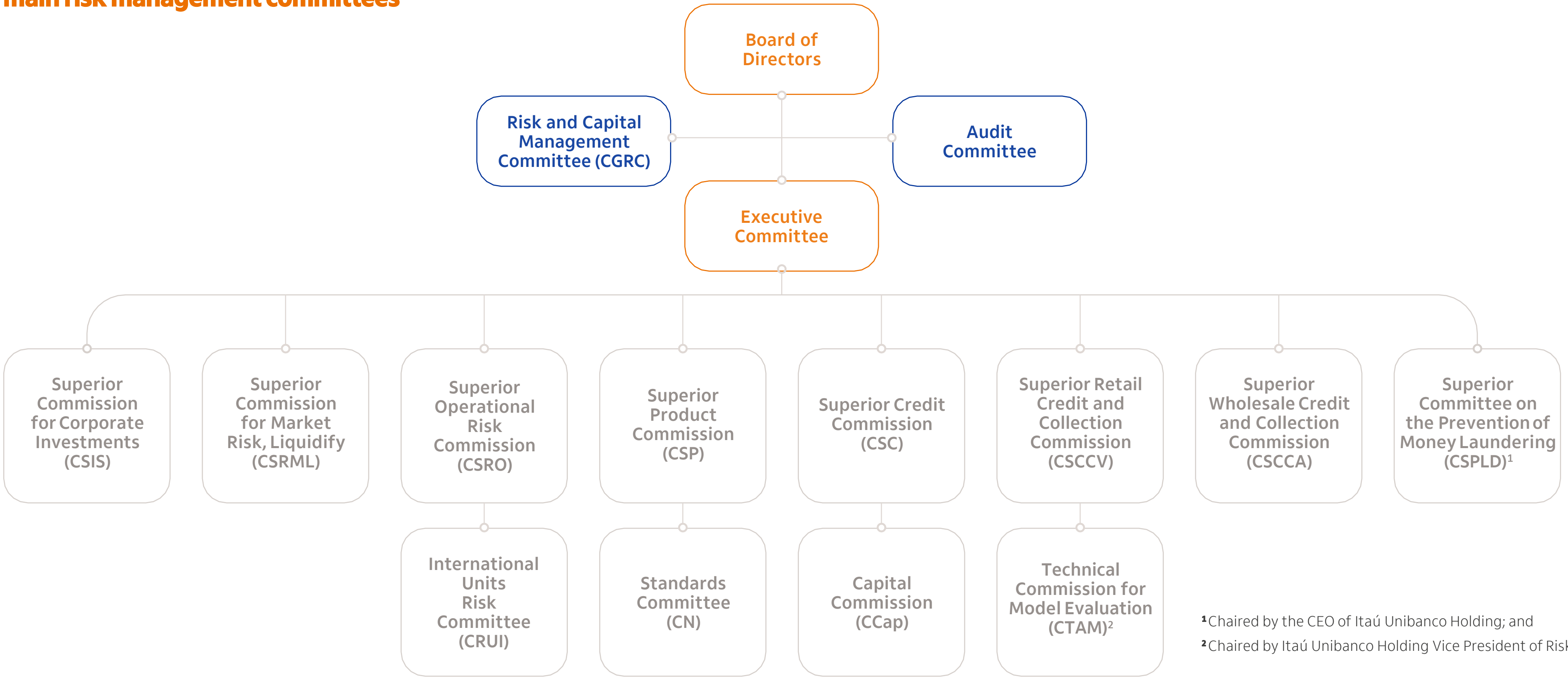
Ricardo Guerra
Technology

[1] Board of Directors independent member.

The Central Bank adopts the same indicators set out by the Basel Committee to determine if Brazilian financial institutions qualify as Global Systemically Important Banks (G-SIBs).

This assessment is required of banks with total exposure—the denominator for the leverage ratio—in excess of EUR200 billion, individually. However, no additional loss absorbency requirements for Brazilian G-SIFIs have been established. We were not included on the latest list of G-SIFIs issued on November 23, 2021, by the Financial Stability Board (FSB). The next update is expected in November 2022.

## main risk management committees




[1] Chaired by the CEO of Itaú Unibanco Holding; and

[2] Chaired by Itaú Unibanco Holding Vice President of Risk.

## risk governance at foreign subsidiaries

Our foreign subsidiaries follow the risk management and governance model established by the holding in its policies and guidelines, keeping an effective flow of information on risk levels between headquarters and each subsidiary and alignment of strategies for maintaining such risks at an acceptable level.

To ensure the continuous improvement of the units' risk management and controls, we implemented a maturity program, comprising the definition and periodic assessment of risk management and control best practices conducted in each location, and also the supervision and governance activities performed by the holding company.

The monitoring proximity of our units allows us to better understand the peculiarities of each country and region where we do business with and quickly adapt to changes in the different regulatory, social, and economic environments where we operate, even in stress scenarios.

These actions to strengthen the risk culture abroad has allowed us to meet the goals of reinforcing the individual and collective responsibility of all employees, so that they can do the right thing, at the right time, and in the right way, respecting our ethical and sustainable way of doing business.

## key risk factors

The Company's risk factors are the list of the risks we consider material to our business and to investments in our securities. Should any of the following risks actually occur, our business and financial position, as well as the value of any investments made in our securities, will be adversely affected. Accordingly, investors should carefully assess the risk factors described below and the information disclosed in this annual report before making an investment decision. The risks described below are those that we currently believe may adversely affect us.

### risks relating to our businesses

Changes in economic conditions may adversely affect us. Our operations depend upon the performance of the economies of the countries in which we do business, in particular Latin American countries. Disruptions and volatility in the international economic environment and the global financial markets may have significant consequences in the countries in which we operate, such as increased volatility in the prices of securities, interest rates, and foreign exchange rates. Increased uncertainty and volatility may result in a slowdown in the credit market and the economy, which, in turn, could lead to higher unemployment rates and a reduction in the purchasing power of consumers, which may adversely affect our business and results of operations.

Geopolitical variables may negatively affect us, such as the recent action of Russian military forces in Ukraine, increasing tensions between Russia and the United States, the North At- lantic Treaty Organization ("NATO"), the European Union, and the United Kingdom. A number of financial and economic sanctions have been imposed on Russia, adversely impacting regional and global financial markets, for example, increasing the price of many commodities, disrupting distribution chan- nels, and increasing prices and inflation across countries.

Changes in applicable laws or regulations may have a material adverse effect on our business. Changes in the laws or regulations applicable to financial institutions in Brazil, as well interpretations of laws by courts and regulators, may affect our ability to grant loans and collect debts in arrears, which may have an adverse effect on us.

Changes in the profile of our business may adversely affect our loan portfolio In addition, the value of any collateral securing our loans may not be sufficient, and we may be unable to realize the full value of the collateral securing our loan portfolio. While the quality of our loan portfolio is associated with the default risk in the sectors in which we operate, changes in our business profile may occur due, among other factors, to our organic growth, merger and acquisition activity, changes in local economic and political conditions, a slowdown in customer demand, an increase in market competition, the outbreak of communicable diseases, such as COVID-19 and other variants.

We face risks relating to the liquidity of our capital resources. Our funding capacity and funding cost may be impacted by a number of factors, such as changes in market conditions (e.g., in interest rates), credit supply, regulatory changes, systemic shocks in the banking sector, and changes in how the market perceive us.

We are exposed to failures, deficiency or inadequacy of our internal processes, human error or misconduct and cyberattacks. Additionally, we rely on third-party services. All these factors may adversely affect us. Due to the high volume of daily processing, we are dependent on technology and management of information, which expose us to eventual unavailability of systems and infrastructure such as power outages, interruption of telecommunication services, and generalized system failures, as well as internal and external events that may affect third parties with which we do business or that are crucial to our business activities and events resulting from wider political or social issues or unauthorized disclosures of personal information in our possession. As a result of the COVID-19 pandemic, we have rapidly increased the number of employees working remotely. This may cause increases in the unavailability of our systems and infrastructure, interruption of telecommunication services, generalized system failures and heightened vulnerability to cyberattacks. Accordingly, our ability to conduct our business may be adversely impacted.

Failure to protect personal information could adversely affect us. We manage and hold confidential personal information of clients in the ordinary course of our business. Even though we have procedures and controls to safeguard personal information in our possession, unauthorized disclosures or security breaches could subject us to legal action and administrative sanctions as well as damage that could materially and adversely affect our operating results, financial position and prospects.

Failure to protect ourselves against risks relating to cyber- security could materially and adversely affect us. We face various cybersecurity risks, including but not limited to: penetration of our information technology systems and platforms, by ill-intentioned third parties, infiltration of malware (such as computer viruses) into our systems, contamination (whether intentional or accidental) of our networks and systems by third parties with whom we exchange data, unauthorized access to confidential client and/ or proprietary data by persons inside or outsideof our organization, and cyber-attacks causing systems degradation or service unavailability that may result in business losses.

The loss of senior management, or our ability to attract and maintain key personnel, could have a material adverse effect on us. Our ability to maintain our competitive position and implement our strategy depends on our senior management. The loss of some of the members of our senior management, or our inability to maintain and attract additional personnel, could have a material adverse effect on our operations and our ability to implement our strategy.

Our business strategy may not provide us the results we expect. Our strategy and challenges are determined by management based on related assumptions, such as the future economic environment, and the regulatory, political and social scenarios in the regions where we do business. These assumptions are subject to inaccuracies and risks that might not be identified or anticipated. Accordingly, the results and consequences arising from any possible inaccurate assumptions may compromise our capacity to fully or partially implement strategies, as well as to achieve the results and benefits expected therefrom, which might give rise to financial losses and reduce the value creation to our stockholders.

Unfavorable court decisions involving material amounts for which we have no or partial provisions or in the event that the losses estimated turn out to be significantly higher than the provisions made, may adversely affect our results and financial position. As part of the ordinary course of our business, we are subject to, and party to various civil, tax and labor lawsuits, which involve substantial financial risks. It is currently not possible to estimate the amount of all potential costs that we may incur or penalties that may be imposed on us other than those amounts for which we have reserves.

We make estimates and assumptions in connection with the preparation of our financial statements, and any changes to those estimates and assumptions could have a material adverse effect on our operating results. These estimates and assumptions are subject to significant uncertainties, some of which are beyond our control. Should any of these estimates and assumptions change or prove to have been incorrect, our reported operating results could be materially and adversely affected.

We face risks associated with the increasingly competitive environment, and recent consolidations in the Brazilian banking industry, as well as competition based on technological alternatives to traditional banking services. Competition has increased as a result of recent consolidations among financial institutions in Brazil and of regulations that (i) increase the ability of clients to switch business between financial institutions, (ii) with the client's permission, grant access to financial and personal information in such institutions, and (iii) establish rules for an instant payment system.

## risks relating to Brazil

Brazilian authorities exercise influence on the Brazilian economy. Our operations are highly dependent upon the performance of the Brazilian economy The demand for credit and financial services, as well as our clients' ability to make payments when due, is directly impacted by macroeconomic variables, such as economic growth, income, unemployment, inflation, and fluctuations in interest and foreign exchange rates. Changes in tax, monetary, and foreign exchange policies as well as a deterioration of government fiscal accounts, may adversely affect us. All fees charged by means of payment to individuals are regulated by BACEN, which may reduce our source of revenue.

### environmental, social and climate risk

We can face financial losses and damages to our reputation that are associated with social and environmental risks Environmental and social risk is considered a material issue for our business, since it can affect the creation of shared value in the short, medium and long terms, from the standpoint of our organization and our main stakeholders, especially in the case of serious environmental and social incidents, including climate risks. Climate risks encompass both physical risks, arising from changes in climate patterns such as rainfalls and temperature rise and extreme weather events; and transition risks arising from economic shifts occurred as a consequence of climate action such as carbon pricing, climate regulation, market risks, reputation risks, and climate litigation. Given their materiality, climate risk has become one of our main priorities.

### risks relating to holders of ADRs (American Depositary Receipts)

Our preferred shares are traded on the New York Stock Exchange in the form of ADRs (one ADR represents one preferred share) and the relative price volatility and limited liquidity of the Brazilian capital markets may significantly limit our investors' ability to sell the preferred shares underlying our ADRs at the price and time they wish. In addition, the cancellation of ADRs could result in the loss of the ability to remit foreign currency abroad and certain tax advantages in Brazil.

## emerging risks

Emerging risks are those with a potentially material impact on the business in the medium and long terms, but for which there are not enough elements yet for their complete assessment and mitigation due to the number of factors and impacts not yet totally known. Their causes can be originated by external events and result in the emergence of new risks or in the intensification of risks already monitored by the Bank.

Emerging risks management process consists of identifying, assessing, and monitoring emerging trends and issues, enabling proper management and allowing preventive measures to be applied to avoid their materialization, mitigating adverse effects, and maximizing opportunities.

The identification and monitoring of Emerging Risks are ensured by the Banks's governance, allowing these risks to be incorporated into risk management processes too. Currently, among the main risks monitored as emerging by the Bank, we highlight cyber security risk; risks related to climate change and new geopolitical events deteriorating macroeconomic conditions.

Learn more about Risk and Capital Management in the Complete financial statements in IFRS

## climate change

We understand climate risk to represent the possibility of losses arising from events of climate origin related to our activities, whether arising from our business with counterparties, our relationships with suppliers, or even from our own operations.

Climate risks represent the possibility of losses arising from events of climate origin related to our activities, whether arising from our business with counterparties, relationships with suppliers, or even from our own operations.

Climate change imposes challenges to our business over different time horizons in credit granting as well as in products and services development. Climate litigation is another key risk whose impacts are still arduous to anticipate, potentially affecting our institution directly and/or our clients, especially in Latin American jurisdictions.

Considering that science, data and tools are not yet sufficient to estimate risks accurately, legislators have a key role in developing public policies that should have echo within regulators who have a role to play in avoiding deficient outcomes by seeking a better understanding of Climate-related risks and by developing scenario-based analysis and guidance.

Climate Change has been discussed into new regulations and standards for the financial sector, reflecting how relevant the topic is for global financial stability.

Climate-change risks can materialize and affect the Bank in several ways. Risks related to public policies, regulatory, technological, market or reputational changes, which arise on the way to a low carbon economy, may incur in costs or change in revenue due to the deterioration of the portfolio's credit quality and climate exposure; change in pricing of assets and real estate; climate regulations and regulator supervision; risk management and governance requirements; disclosure obligation; climate litigation, such as stranded assets and credit underwriting; carbon pricing; carbon reduction, neutralization and removal; cost of emissions; change in legislation; market barriers and stakeholder requirements; adaptation and training (including expertise at board and CE level).

Further, climate-related court decisions may impose emerging risks since courts interpretations and rules may vary, even potentially imposing further obligations not yet identified for a financial institution.

Acknowledging climate risks and their potential impacts is an important step in defining our climate strategy. As recommended by TCFD, we evaluate the impact of climate risks regarding their possible materialization period and classifying then according to their nature and possible qualitative materialization scenarios.

We periodically assess the sensitivity of our portfolio to climate risks and report the results to the relevant forums in accordance with our Climate Risk Management Procedure.

We implemented 100% of projects in response to the TCFD recommendations and worked on the transition to a low carbon economy, including by defining policies and action plans. Our goal is to become a Net Zero Carbon bank by 2050.

We also have identified our exposure to climate-related risks considering the results of our exercise applying PCAF´s methodology to measure financed emissions, as well as the benefits of using PACTA´s directions to measure the alignment of our credit portfolio with the Paris Agreement.

Additionally, reputational risk elements comprise wholesale banking´s credit grating decisions, our practices include not potential climate-related legal issues that may be imposed to some clients and deals (potential lawsuits), but also take into consideration our own commitments to join efforts in response to the global climate emergency. We support key guidelines and commitments and monitor public consultation regarding climate related disclosures, such as IFRS an ISSB.

Learn more about Climate Change in the ESG Report 2021.

## cyber security

Our commitment is always to address this topic rigorously by adopting the measures necessary for the security and privacy of our clients, employees and other personal data owners.

We are subject to cyber security risks, such as the invasion of our systems and platforms by third parties acting in bad faith, infiltration of our systems by malware (such as computer viruses), contamination (intentional or accidental) of our networks and systems by third parties with whom we exchange information, unauthorized access to confidential information on clients and/or proprietary information by people from inside or outside the organization, and cyber-attacks.

We are exposed to this risk over the entire lifecycle of the information, from the moment it is collected until its processing, transmission, storage, analysis and destruction.

A successful cyber-attack can result in the unavailability of our services, or the data breach, which may cause unauthorized access and the loss of significant volumes of client data and other critical information. As attempted attacks increase in scope and sophistication, we may incur significant costs to change or improve our protection measures or to investigate and correct any vulnerability or breach.

There has been a significant increase in the volume of cyber-attacks as result of several global factors that directly impact this scenario, such as the degradation of the socioeconomic environment aggravated by the COVID-19 pandemic, which has result in an increase of to the volume of employees working in home office that facilitates the grooming carried out by hackers and the increase in the activity of cybercriminal groups.

A publication released by the Flashpoint and Risk Based Security observed that over 63% of breaches occurring within the financial services sector originate from "hacking," or unauthorized access to systems or services. Whether or not these incidents stem from outside or inside the organization, the type of data that is being targeted remains consistent. Threat actors, including insiders, typically target names, Social Security Numbers (SSNs), as well as other financial data, including bank account numbers and transaction details, with the purpose of using them in phishing attacks, committing fraud, or selling them on illicit forums and marketplaces.

Information security management for cybersecurity seeks to prevent breaches of our data, minimize risks of service unavailability, protect integrity and prevent information leakage. To this end, we use an expanded perimeter protection strategy, a concept that believes that the information must be protected wherever it is - within the Bank's infrastructure, in a cloud service at a service provider or at an international unit - considering the entire lifecycle of the information.

We adopted strict control processes aimed at detecting, preventing, ongoing monitoring and immediately responding to attacks and attempted hacking of our infrastructure, thus ensuring security risk management and building a strong foundation for an increasingly digital future.

Our monitoring processes are constantly improved and updated, allowing for the identification and performance of preventive and increasingly efficient measures, which are compatible with the evolution of the cyber threat environment. To ensure that everything is in accordance with the planning, we carry out independent tests using reputable cyber security companies, and our controls are checked by independent external audit firms every year.

In order to anticipate new threats, we continue to expand our work on intelligence about virtual threats, and also actively participate in cyber security forums of the industry and the Government to strengthen our defenses. Other important issue is discussions about risk and attack events that take place via the Financial Services Information Sharing and Analysis Center (FS-ISAC).

Additionally, we have a robust and friendly awareness raising program, with training to emphasize the importance of privacy, data protection and cyber security throughout the institution, with initiatives to disseminate and promote engagement with and knowledge of the topic to employee, customers and public in general.

The financial ecosystem faces challenges in finding the balance between fighting cybercrime and continuing to support digital transformation and emerging technologies, while strengthening its defenses and complying with current regulations.

Learn more about cybersecurity in the ESG Report 2021.

## new geopolitical events deteriorating macroeconomic conditions

Geopolitical events, which emerge from conflict between nations, might change economic conditions and adversely affect us.

Our operations depend upon the performance of the economies of the countries in which we do business, in particular Latin American countries and specially in Brazil, and those economies are susceptible to the international economic environment.

The recent actions of Russian military forces in Ukraine, for example, increased tensions between Russia and the United States, European Union and UK. Several financial and economic sanctions have been imposed on Russia, adversely impacting regional and global financial markets, increasing the price of commodities, disrupting distribution channels, and increasing prices and inflation across countries.

Disruptions and volatility in the global economic environment and financial markets may have significant consequences in the countries in which we operate, such as increased volatility in the prices of securities, interest rates, and foreign exchange rates. Increased uncertainty and volatility may result in a slowdown in the credit market and the economic growth, which, in turn, could lead to higher unemployment rates and a reduction in income and the purchasing power of consumers, which may adversely affect our business and results of operations. The demand for credit and financial services, as well as our clients' ability to make payments when due, is directly impacted by those macroeconomic variables.

Members of the Board of Directors and the Board of Officers of IUH are professionals of proven knowledge in the capital markets area. They proactively adjust strategic guidelines to reflect significant changes in the macroeconomic scenario.

Predicting new geopolitical disruption is difficult, however IUH performs constantly improving stress tests, a framework for severe scenarios brainstorm, design, analysis, and outcome measurement, evaluating the potential impact on its portfolios, capital, and liquidity.

Additionally, the alignment of strategies with our foreign subsidiaries and monitoring through periodic assessment of risk management and controls, allows us to better understand the peculiarities of each country where we operate and quickly adapt to changes in those economic environments