



## **GUIDELINES ON THE INTERNAL CAPITAL ADEQUACY ASSESSMENT PROCESS (“ICAAP”)**

### **SECTION I GENERAL PROVISIONS**

#### **Article 1**

##### **Introduction**

1. The best international practices on banking supervision are established by the Basel Committee on Banking Supervision (BCBS), which is the primary global standard setter for the prudential regulation of banks and has defined three pillars for Capital Measurement and Capital Standards, all consolidated in the document “The Basel Framework”, available at the BIS - Bank of International Settlement website.
2. The Instruction 21/2023 dated July 04, on Regulatory Capital and Leverage Ratio has regulated Pillar 1 in Timor-Leste, and set the minimum risk weighted capital requirements for credit risk, market risk and operational risk.
3. The Article 30 of the above-mentioned Instruction has also required banks to adopt an internal capital adequacy assessment process (ICAAP) and prepare an ICAAP report to be submitted to the BCTL, for a supervisory review and examination process (SREP), to ensure that banks have adequate capital and liquidity to support all the risks in their business, especially with respect to risks not fully captured by the Pillar 1 process and to encourage good risk management.
4. Such requirement corresponds to Pillar 2 of Capital Measurement and Capital Standards, and its objective is to ensure that the capital held by the bank is adequate for the bank's overall risk profile. This includes, among other factors, the effectiveness of the bank's risk management systems in identifying, assessing, and measuring, monitoring and managing the various risks, including interest rate risk in the banking book, liquidity risk, concentration risk and risk residual risks, as referred in Article 31 of the same Instruction.
5. Pillar 3 is related to market discipline and disclosure of information and has been covered by requirements of Instruction 23/2023, on the Chart of Accounts and Instruction 24/2023, on Reporting and Publication, both dated July 04.
6. The objective of this Guidelines is to ensure convergence of sound practices for the preparations of banks' internal capital adequacy assessment process (ICAAP) and the supervisory review and evaluation process (SREP) in accordance with the above-mentioned Instruction BCTL n° 21/2023.
7. The Guidelines are written based on Pillar 2 of the Basel Framework and taking into account the characteristics of the financial system in Timor-Leste.

8. These guidelines are aimed at assisting banks in strengthening their ICAAP and at encouraging the use of best practices by providing details of the BCTL expectations on the ICAAP, leading to more consistent and effective supervision.
9. In accordance, Banks shall have a process for assessing their overall capital adequacy in relation to their risk profile and a strategy for maintaining their capital levels.
10. BCTL should review and evaluate the bank's internal capital adequacy assessments and strategies, as well as their ability to monitor and ensure their compliance with the regulatory capital ratios and should take appropriate supervisory action when not satisfied with the results, which is denominated supervisory review and evaluation process (SREP).
11. The guidelines do not substitute for or supersede the Regulation 2000/8 or applicable BCTL Instructions. When the guidelines are not in line with those documents, the referred documents must prevail.

## **Article 2**

### **Definitions**

1. In this Guideline, unless reasonably implied by contextual usage, the following expressions and words shall mean:
  - b) **"Internal Capital Adequacy Assessment Process (ICAAP)"**: the bank's process for the identification, measurement, management and monitoring of internal capital considered adequate to cover all material risks to which it is exposed.
  - c) **"Supervisory Review and Evaluation Process (SREP)"**: the process of the regular review of bank's strategies, processes and mechanisms implemented and the evaluation of risks to which the banks are or might be exposed, or poses risk to the financial system
  - d) **"Risk appetite"**: the aggregate level and types of risk the bank is willing to assume within its risk capacity, in line with its business model, to achieve its strategic objectives.
2. Other terms referred to the document have already been defined by Regulation 2000/8, of February 25, on Banking Licensing and Supervision or by previous BCTL Instructions or Guidelines.

## **Article 3**

### **Purpose and Scope**

1. These Guidelines provide directions for banks in Timor-Leste to establish, operate, and report their Internal Capital Adequacy Assessment Process (ICAAP) in accordance with Basel III and applicable IFRS standards.
2. The purpose of the Internal Capital Adequacy Assessment Process (ICAAP) is to inform the Board of Directors of the ongoing assessment of the bank's risks, how the bank intends to mitigate those risks and how much current and future capital is necessary having considered other mitigating factors.
3. The guidelines apply to all banks and other deposit taking institutions licensed to operate in accordance with Regulation 2000/8.
4. Branches of foreign banks shall prepare an ICAAP analyzing the capital allocated to the branch and the capital requirements taking into account the risks assumed by the branch.
5. Each bank is responsible for its ICAAP.

## **Article 4**

### **Guiding principles for ICAAP**

1. The ICAAP is intended not only to ensure that banks have adequate capital to support all the risks in their business, but also to encourage banks to develop and apply improved risk management techniques in monitoring and managing their risks. Banks must have a process for assessing their overall capital adequacy in relation to their risk profile and a strategy for maintaining their capital levels.
2. The ICAAP shall ensure that banks maintain sufficient capital to support their risks, with processes proportional to the size, nature, and complexity of their operations
3. ICAAP must explicitly incorporate Basel III capital buffers, including the Capital Conservation Buffer (CCB), Countercyclical Capital Buffer (CCyB), and, where applicable, Systemic Risk Buffers. Banks shall ensure that capital planning maintains compliance with these buffers in both baseline and stressed conditions.
4. The Board of Directors, Senior Management, and relevant risk committees bear ultimate responsibility for ICAAP. These bodies must ensure the design, implementation, and ongoing operation of ICAAP are aligned with the Bank's strategy, risk appetite, and regulatory obligations. The bank management has the responsibility for developing an internal capital assessment process and setting capital targets that are commensurate with the bank's risk profile and control environment. The bank management bears the responsibility for ensuring that the bank has adequate capital to support its risks beyond the core minimum requirements.
5. ICAAP shall be proportional to the size, nature, complexity of the bank's business, risk profile, and operating environment.
6. BCTL considers that a relationship exists between the amount of capital held by the bank against its risks and the strength and effectiveness of the bank's risk management and internal control processes. However, increasing capital levels is not the sole solution to rising risks; other mitigation strategies, such as strengthening risk management or internal controls, enhancing provisions and reserves, and refining limits, can also be employed.
7. A bank must maintain sound, effective, and comprehensive strategies and procedures to continuously assess and manage the levels, composition, and allocation of internal capital adequate to support its material risks.
8. There are three main areas that must be covered under Pillar 2 and contemplated in the ICAAP:
  - a). risks considered under Pillar 1 but not fully captured by the Pillar 1 process, as credit concentration risk;
  - b). risks not included in the Pillar 1 process, as interest rate risk in the banking book or business and strategic risks; and
  - c). external factors to the bank, such as macroeconomic or business cycle effects.
9. A relevant aspect of Pillar 2 is to ensure compliance with the minimum standards set by Instruction 21/2023 on Regulatory Capital and Leverage, and applicable disclosure requirements related to advanced approaches under Pillar 1. A bank must ensure that those requirements are being met, both as qualifying criteria and on a continuing basis.
10. Banks will need to implement this guideline based on the following key principles:
  - a). Management bodies bear the responsibility for ICAAP. The Board of Directors, Senior Management and risk committees need to take full ownership of the processes and also of the capital adequacy statement.

- b). The ICAAP is part of the risk management framework, and the processes shall be aligned with group risk appetite and look not just at the current situation.
- c). The ICAAP shall cover a planning horizon of at least three years to ensure the bank's short and medium-term viability.
- d). Banks need to make their assessments from two complementary perspectives:
  - i. **The normative perspective** that ensures compliance with the supervisory requirements, including key ratios such as CET 1, Tier 1, CAR, and leverage, considering the short-term position but also looking forward three years or more, including a baseline scenario and at least two adverse scenarios.
  - ii. **The economic perspective** that assesses the bank's economic value or net present value, considering risks as a potential shareholder, who would include 'hidden' or off-balance sheet liabilities into account.
- 11. The ICAAP shall identify and consider all material risks. Banks are expected to address any potential threats to their capital or liquidity positions, according to their business model. Appropriate systems and procedures shall be in place to ensure continuous monitoring and management of risks, ensuring capital and liquidity levels remain adequate relative to the Bank's risk profile.
- 12. Capital needs to be clearly defined, and of high quality, with a predominant role assigned to Common Equity.
- 13. ICAAP assumptions and methodologies must be:
  - a). Proportionate to the bank's size and complexity.
  - b). Appropriate to business lines and risk appetite.
  - c). Independently validated and regularly reviewed.
  - d). Conservatively calibrated.
- 14. A bank must conduct regular and comprehensive internal stress tests - at least annually - based on plausible but adverse scenarios. Stress testing must inform ICAAP and capital planning processes, supporting resilience in periods of market stress.
- 15. Banks should also conduct reverse stress testing, identifying scenarios that would render their business model unviable, to inform recovery and resolution planning.

## SECTION II

### RISK MANAGEMENT REQUIREMENTS

#### Article 5

##### Process

- 1. BCTL has been regulating the management of the most relevant risks affecting a bank in Timor-Leste. Instructions on the management of credit risk and liquidity risk have already been issued. Other instructions are being prepared. While not in place, banks can use the summary under these Guidelines, the literature and the Basel Framework for consideration of other risks.
- 2. Sound risk management processes are necessary to support supervisory and market participants' confidence in banks' assessments of their risk profiles and internal capital adequacy assessments.
- 3. A sound risk management system should have the following key features:
  - a) Board of Directors and Senior Management oversight.
  - b) Established policies, procedures, limits and controls;

- c) Identifying, measuring, monitoring and reporting key risks;
- d) A comprehensive assessment of risks; and
- e) Internal control review.

## **Article 6**

### **Responsibilities**

1. It is the responsibility of the Board of Directors and Senior Management to define the institution's risk appetite and to ensure that the bank's risk management framework includes detailed policies that set specific firm-wide prudential limits on the bank's activities, which are consistent with its risk-taking appetite and capacity.
2. In order to determine the overall risk appetite, the Board and Senior Management must first have an understanding of risk exposures on a firm-wide basis.
3. Senior Management should establish a risk management process that is not limited to credit, market, liquidity and operational risks, but incorporates all material risks. This includes reputational, legal and strategic risks.
4. A sound risk management process is the foundation for an effective assessment of the adequacy of a bank's capital position. Bank management is responsible for understanding the nature and level of risk being taken by the bank and how this risk relates to adequate capital levels. Senior Management and the Board of Directors must view capital planning as a crucial element in being able to achieve its desired strategic objectives.
5. The Board of Directors and Senior Management shall ensure that capital planning is aligned with risk appetite, strategic goals, and supervisory requirements.
6. The Board and Senior Management shall ensure that capital planning is fully integrated with recovery and resolution planning, consistent with Basel III principles on going concern and gone concern capital adequacy.
7. The Board of Directors and Senior Management must:
  - a) possess sufficient knowledge of all major business lines to ensure that appropriate policies, controls and risk monitoring systems are effective;
  - b) have the necessary expertise to understand the capital markets activities in which the bank is involved and the associated risks;
  - c) remain informed on an on-going basis about these risks as financial markets, risk management practices and the bank's activities evolve;
  - d) ensure that accountability and lines of authority are clearly delineated;
  - e) understand the underlying assumptions regarding business models, valuation and risk management practices for new or complex products;
  - f) ensure that accountability and lines of authority are clearly delineated;
  - g) identify and review the changes in bank wide risks arising from potential new products or activities before embarking on new activities or introducing new products to the bank;
  - h) ensure that the infrastructure and internal controls necessary to manage the related risks are in place; and
  - i) be satisfied that all business units conducting activities that have an impact on liquidity are fully aware of the capital and liquidity management strategy and operate in accordance with approved policies, procedures, limits and controls.

8. The risk management function of banks must be independent of the business lines in order to ensure an adequate separation of duties and to avoid conflicts of interest. Banks must ensure that its risk function and its Chief Risk Officer (CRO) or equivalent person reports directly to the Board of Directors and the Chief Executive Officer (CEO).
9. The risk function must be highlighted by the Board of Directors and Senior Management risk management concerns such as risk concentration and breaches of tolerable risk limits.

## **Article 7**

### **Policies, Procedures, Limits and Controls**

A bank's policies, procedures and limits should:

- a) provide for adequate and timely identification, measurement, monitoring, control and mitigation of the risks posed by its lending, investing, trading, securitization, off balance sheet, fiduciary and other significant activities at the business line and firm wide levels;
- b) ensure that the economic substance of a bank's risk exposures, including reputational risk and valuation uncertainty, are fully recognized and incorporated into the bank's risk management processes;
- c) be consistent with the bank's stated goals and objectives, as well as its overall financial strength;
- d) clearly delineate accountability and lines of authority across the bank's various business activities, and ensure there is a clear separation between business lines and the risk function;
- e) escalate and address breaches of internal position limits;
- f) provide for the review of new businesses and products by bringing together all relevant risk management, control and business lines to ensure that the bank is able to manage and control the activity prior to it being initiated; and
- g) include a schedule and process for reviewing the policies, procedures and limits and for updating them as appropriate.

## **Article 8**

### **Identifying, measuring, monitoring and reporting key risks**

1. Effective risk monitoring requires institutions to identify and measure all material risk exposures. Consequently, risk monitoring activities must be supported by strong management information systems (MIS).
2. To support the effective measurement and monitoring of risks, banks should adhere to the following principles:
  - a) Risk monitoring practices and reports must comprehensively address all material risks faced by the institution.
  - b) Key assumptions, data sources, and methodologies used for risk measurement and monitoring should be suitable, thoroughly documented, and regularly tested for reliability.
  - c) Reporting and communication mechanisms should align with the institution's activities, be designed to track exposures and ensure compliance with established limits, goals, or objectives, and, where applicable, compare actual performance against expectations.

- d) Reports submitted to management and the board of directors must be accurate, timely, and sufficiently detailed to enable informed decision-making, identification of adverse trends, and assessment of the institution's risk profile.
- 3. A bank's Management Information System (MIS) must provide the board and Senior Management with clear, concise, timely, and relevant information regarding the institution's risk profile. This information should include all risk exposures, including off-balance sheet items.
- 4. The key components necessary for effective risk aggregation are a robust infrastructure and MIS that:
  - a) Allow for the aggregation of exposures and risk measures across business lines; and
  - b) Support the customized identification of risk concentrations and emerging risks.
- 5. A bank's MIS should be capable of detecting limit breaches, with procedures in place to promptly report such breaches to Senior Management and ensure appropriate follow-up actions are taken. For example, similar exposures should be aggregated across business platforms (including the banking and trading books) to determine whether a concentration exists, or an internal position limit has been breached.
- 6. The MIS should support the ability to evaluate the potential impact of various economic and financial shocks on the institution as a whole.
- 7. To enable proactive risk management, the board and Senior Management must ensure that the MIS provides regular, accurate, and timely information on the bank's aggregate risk profile, along with the key assumptions used in risk aggregation.
- 8. The MIS should be adaptable and responsive to changes in the bank's underlying risk assumptions. It should incorporate multiple perspectives of risk exposure to reflect uncertainties in measurement. Furthermore, it must be sufficiently flexible to support forward-looking, institution-wide scenario analyses that capture management's interpretation of evolving and stressed market conditions.
- 9. Third-party inputs or tools used within the MIS (e.g., credit ratings, risk measures, models) must be subject to initial and ongoing validation.

## **Article 9**

### **Comprehensive Assessment of Risks**

- 1. The Board of Directors and Senior Management should promote the identification, assessment, and management of data-quality risks within the bank's overall risk management framework. The framework should include service-level standards and policies covering data confidentiality, integrity, availability, and risk management.
- 2. All material risks faced by the bank should be addressed in the capital assessment process. Even though some risks cannot be measured precisely, a process should be developed to estimate risks. Therefore, at least the risk exposures discussed in the following section should be considered.
- 3. The Board should also review and approve the group risk data aggregation and risk reporting framework, and ensure adequate resourcing. The risk data aggregation and reporting practices must be fully documented and subject to independent, high-standard validation. Validation must be aligned with internal control functions and performed by staff with IT, data, and reporting expertise.
- 4. The Senior Management must understand limitations of current data aggregation and commit to remediation via strategic IT planning. Critical data and infrastructure should be identified and supported through appropriate financial and human resource allocation.
- 5. The board must define its risk reporting requirements, understand data aggregation limitations, and ensure compliance with regulatory principles.

6. Risk data must be aggregated accurately and reliably, using controls comparable to those for accounting data. Where manual processes are used, robust mitigants must be implemented.
7. Risk data must be reconciled with source systems, including accounting data. Banks should aim for a single authoritative source for each risk type. Risk personnel must have sufficient access to validate and reconcile risk data. A comprehensive data dictionary must be maintained as well as a balanced use of automation and manual intervention, with a preference for automation where it is possible to reduce error.
8. All aggregation processes should be documented, especially manual workarounds, and assessed their criticality. Measurement and escalation mechanisms should be established to monitor and address data accuracy deficiencies.
9. Assessment of risks must encompass all material exposures, including off-balance sheet items. While aggregation systems may differ, they must allow for consistent capability across risk types. Each system must clearly define its aggregation approach to enable informed oversight by the board and management. Banks must ensure the completeness of aggregated data and monitor for deficiencies. Any incompleteness must be non-critical and fully documented with appropriate justification.
10. Banks must be able to produce aggregated risk information promptly to meet all internal and regulatory risk reporting requirements. Banking systems must support the rapid generation of aggregated data during stress or crisis situations for all critical risk categories, including:
  - a) Large corporate credit exposures
  - b) Counterparty credit risk (e.g., derivatives)
  - c) Trading exposures and market concentrations
  - d) Liquidity indicators (e.g., cash flows, funding)
  - e) Operational risk indicators (e.g., system availability)
11. Banks must ensure their systems are adaptable to ad hoc risk data requests and emerging risk assessments. Adaptability includes:
  - a) Flexible aggregation processes for rapid analysis and decision-making;
  - b) User-specific customization (dashboards, drilldowns, summaries);
  - c) Integration of new organizational or external risk developments; and
  - d) Accommodation to regulatory changes
12. Banks must generate specific data subsets quickly, such as country credit exposures by list and date or industry exposures across business lines and geographies.
13. Risk reports must be accurate and precise to support critical decision-making by the board and Senior Management. Banks must implement control mechanisms like:
  - a) Defined reconciliation processes for aligning reports with source data;
  - b) Automated/manual validation checks with a documented rule inventory; and
  - c) Integrated processes for exception identification and reporting.
14. Where approximations (e.g., models, stress tests) are used, accuracy expectations must be established and governed by internal standards. Accuracy standards should reflect the materiality of omissions or misstatements, guided by internal validation and reconciliation results.
15. Reports must cover all significant risks (e.g., credit, market, liquidity, operational) and relevant components (e.g., industry, geography). Reports should highlight concentrations and alignment with risk appetite and recommend mitigating actions. They should also provide forward-looking insights using forecasts and stress testing.

16. Reports must enable effective risk decisions at all governance levels and be tailored to recipient needs. Reports should balance:
  - a) Quantitative and qualitative data
  - b) Aggregated summaries and contextual interpretation
  - c) Details appropriate to the organizational level of the user
17. The board must define and periodically review its reporting requirements. Senior Management must ensure it receives suitable information for managing risks. Banks must maintain a classification system for reported risk data, with references to underlying concepts and sources.
18. Periodic validation must ensure that reports remain relevant in scope, content, and format to support governance and risk decisions.
19. The frequency of reports must align with risk type, user needs, and intended use. Banks must define and test the required timelines, especially under stress conditions. In stress/crisis scenarios, critical risk data (credit, market, liquidity) must be available within very short timeframes, including intraday reporting where necessary.
20. Banks must implement procedures to collect, analyze, and distribute risk data swiftly, while maintaining appropriate confidentiality. Banks must periodically confirm that all relevant stakeholders receive timely and appropriate risk reports.

#### **Article 10**

##### **Internal Control Review**

1. Risk management processes must be regularly monitored and tested by independent control functions, as well as by internal and external auditors. The objective is to ensure that decision-making is based on accurate information, that processes faithfully reflect management policies, and that reporting—particularly concerning limit breaches and other exception-based events—is conducted effectively.
2. The bank's risk management function must operate independently from business lines to ensure adequate separation of duties and to avoid conflicts of interest.

#### **Article 11**

##### **Compensation Practices**

1. Risk management must be embedded in a bank's culture. It should be a core priority for Senior Management, trading desks, and other business units in both strategic and operational decision-making.
2. To support a robust risk culture, compensation policies must not overly emphasize short-term accounting profits. Instead, they should be aligned with long-term capital preservation and financial strength, incorporating risk-adjusted performance measures. Banks should disclose their compensation policies to stakeholders transparently.
3. The Board and Senior Management are responsible for ensuring that remuneration practices do not undermine firm-wide risk management.

## **Article 12**

### **Valuation Practices**

1. Banks must maintain robust governance frameworks for valuation practices, ensuring consistency, transparency, and effective oversight across the institution. Where observable market inputs are unavailable, internal models must be appropriately calibrated, validated, and documented.
2. Valuation processes must comply with IFRS 13 (Fair Value Measurement) and ensure that valuation adjustments are incorporated consistently into both financial reporting and risk management frameworks.
3. Valuation practices hold a central place in a bank's ability to fairly assess the worth of financial instruments, influencing not only financial reporting but also the measurement and management of risk. Yet, the nature of complex structured products renders valuation an inherently challenging endeavor. This complexity stems from factors such as the absence of active, liquid markets, the intricate and often bespoke structure of cash flow arrangements, and the sensitive interplay between valuation outcomes and underlying risk factors.
4. In the absence of transparent, market-derived prices, valuation must often rely on internal models, proxy-pricing techniques, and the seasoned judgment of experts. Yet these models are deeply dependent on the accuracy and relevance of the assumptions and parameters applied. The calibration of such models is further complicated by the lack of reliable benchmarks in illiquid or thinly traded markets.
5. Given these challenges, banks are expected to maintain strong governance frameworks and control processes around valuation. The structures that guide fair valuation should align seamlessly with those governing risk oversight and financial reporting, ensuring consistency and integrity across the organization.
6. Within this structure, the role of the board and Senior Management must be clearly articulated. The board should be kept informed by senior leadership on matters of valuation oversight, model performance, and any substantial revisions to valuation policies. A clearly delineated governance arrangement should guide the generation, assignment, and independent verification of financial instrument valuations, supported by well-documented approval processes for all valuation methodologies.
7. A bank's control processes for valuation must be consistently applied across all units and integrated into the institution's broader risk management infrastructure. Controls should be uniform across instruments of similar risk characteristics and harmonized across business lines. These controls, crucially, must be subject to internal audit, ensuring they are not only implemented but also scrutinized and upheld.
8. To ensure the robustness of valuations under all conditions, including during market stress, a bank must possess sufficient capacity to maintain and verify valuations. This capacity must be proportionate to the size, complexity, and risk profile of the bank's exposures. Where exposures present significant risk, the bank must be capable of applying alternative valuation methods if primary inputs become unreliable or unavailable due to illiquidity or market disruption.
9. In active markets, the priority should be to rely on observable inputs and minimize reliance on subjective or unobservable ones. However, when markets become inactive, observable inputs may lose relevance, such as in forced sales or during distress. In such cases, accounting guidance may offer direction, but discretion and judgment remain critical.
10. To assess the credibility of a price or source, a bank should weigh factors such as:
  - a) the frequency and accessibility of quotes;
  - b) whether prices reflect actual, arm's-length transactions;

- c) the dispersion and accessibility of data across the market;
- d) the timeliness of the information;
- e) the number of independent data sources;
- f) the presence of supporting transactions;
- g) the maturity and stability of the market; and
- h) the comparability between the referenced transaction and the bank's own instrument.

### **Article 13**

#### **Stress Testing Practices**

1. Stress testing is a critical element of risk management for banks. It is integral to banks' risk management alerting bank management to unexpected adverse outcomes in a variety of risks, and providing an indication of the required financial resources to absorb losses if large shocks occur.
2. BCTL recommend banks to comply with the Stress Testing Principles established by the Basel Committee (Stress testing principles, Basel Committee on Banking Supervision, October 2018, available at [www.bis.org/bcbs](http://www.bis.org/bcbs)). The Principles set out guidance on the core elements of stress testing frameworks, such as objectives, governance, policies, processes, methodology, resources, and documentation that may guide stress testing activities and facilitate their use, implementation and oversight.
3. Stress testing must be embedded as a critical component of sound risk management.
4. The principles are intended to be applied on a proportionate basis, depending on size, complexity and risk profile of the bank or banking sector. Even smaller banks can benefit from considering in a structured way the potential impact of adverse scenarios on their business, even if they are not using a formal stress testing framework but are instead using simpler methods.
5. The Board of Directors must define and formally approve clear, documented objectives for the stress testing framework. Senior Management must ensure that these objectives are communicated throughout the organization and are consistent with the bank's risk appetite and governance framework. All staff involved in implementation must understand these objectives to guide judgmental or discretionary decisions.
6. Senior Management, under oversight from the Board, must implement a comprehensive, documented governance framework for stress testing. They must define roles and responsibilities for scenario design and approval, model development and validation, result analysis and reporting, and oversight by the second and third lines of defense (e.g. Risk Management, Compliance, and Internal Audit). They need also to ensure involvement of all key stakeholders and maintain consistent oversight throughout the stress testing process.
7. The Board of Directors holds ultimate responsibility for the stress testing framework. The Board or designated governance committee must actively engage with Senior Management and stress testing experts, as well as challenge modelling assumptions, scenario choices, and methodological foundations.
8. Senior Management must embed stress testing into the bank's strategic, risk, and policy decision-making processes. Stress testing must support capital and liquidity planning, and contribute to policy setting and long-term business planning.
9. Risk and Finance Functions, under direction of Senior Management, must ensure that stress test results are reported to the Board, or the Risk Management Committee, at defined intervals and levels of aggregation, including scenario assumptions and identified limitations, and that the results are

- used to inform the risk appetite and tolerance levels; the capital and liquidity adequacy assessments; contingency, recovery, and resolution plans; and portfolio management and new product approvals.
10. A risk management function, under Senior Management supervision, must perform a comprehensive assessment of relevant risks, including on/off-balance sheet exposures, operational vulnerabilities and earnings volatility, documenting any exclusions and justifying them explicitly.
  11. A risk and modelling teams, coordinated by Senior Management, must:
    - a) Design scenarios that are internally consistent and aligned with identified material risks;
    - b) Ensure plausibility and severity appropriate to the test's objectives;
    - c) Review scenarios periodically to maintain relevance; and
    - d) Incorporate both historical and forward-looking hypothetical events.
  12. The Senior Management must allocate appropriate resources to execute the stress testing framework, ensuring:
    - a) Sufficient skilled personnel, systems, and IT infrastructure;
    - b) Staff capabilities in risk disciplines (e.g. credit, market, liquidity), accounting, and modelling; and
    - c) Ongoing staff development and/or hiring of specialized personnel.
  13. A data governance function, overseen by risk and finance departments, must:
    - a) Maintain a robust data infrastructure to support stress testing;
    - b) Guarantee data accuracy, completeness, and appropriate granularity; and
    - c) Address data gaps through predefined remediation processes.
  14. A model development team, with input from risk and business units, must define model scope, segmentation, and sophistication aligned with objectives, document and justify all methodologies and assumptions, and reflect interactions between risk types (e.g. solvency and liquidity).
  15. A model validation function, independent from model development, must review model assumptions, overlays, and calibration decisions, and conduct independent validation, providing challenge to modelling processes.
  16. Senior Management must ensure periodic and comprehensive review of all framework components. The review team must validate scenarios and methodologies, conduct sensitivity testing and benchmarking and assess the overall framework adequacy.
  17. The business units, risk management, and oversight bodies must engage in challenge sessions during scenario development, modelling, and reporting phases, evaluating assumptions and outputs at multiple organizational levels.
  18. The internal audit function must regularly review the stress testing framework, both for internal and supervisory tests, and report findings to the Audit Committee with suggestions of corrective actions.

### **SECTION III**

#### **RISKS UNDER PILLAR II**

##### **Article 14**

##### **Credit Risk**

1. Banks must maintain sufficient capital for credit risk exposures under Pillar 1 and address residual risks, concentration risks, and counterparty credit risk through ICAAP.

2. Stress testing must evaluate credit exposures under adverse conditions.
3. Banks must ensure that their credit risk provisioning policies are aligned with IFRS 9 Expected Credit Loss (ECL) requirements.
4. A bank should ensure that it has sufficient capital to meet the Pillar 1 requirements established by Instruction 21/2023, on Regulatory Capital and Leverage Ratio. The Instruction sets a minimum capital requirement for Credit, Market and Operational Risks.
5. The results of the stress test should contribute directly to ensure that a bank will operate above the Pillar 1 minimum regulatory capital ratios. To the extent that there is a shortfall, the bank's Board of Directors should react appropriately, reducing the risks and/or holding additional capital/provisions, so that existing capital resources could cover the Pillar 1 requirements plus the result of a recalculated stress test.
6. **Residual risk**
  - 6.1. The above-mentioned Instruction, in relation to credit risk, allows banks to offset credit or counterparty risk with collateral, guarantees or credit derivatives, leading to reduced capital charges. While banks use credit risk mitigation (CRM) techniques to reduce their credit risk, these techniques give rise to risks that may render the overall risk reduction less effective. Accordingly, these risks (as legal risk, documentation risk, or liquidity risk) to which banks are exposed are of supervisory concern.
  - 6.2. Where such risks arise, and irrespective of fulfilling the minimum requirements set out by the Instruction, a bank could find itself with greater credit risk exposure to the underlying counterparty than it had expected. Examples of these risks include:
    - a) inability to seize, or realize in a timely manner, collateral pledged (on default of the counterparty);
    - b) refusal or delay by a guarantor to pay; and
    - c) ineffectiveness if untested documentation.
  - 6.3. Banks should have in place appropriate written CRM policies and procedures in order to control these residual risks. A bank must regularly review their appropriateness, effectiveness and operation.
  - 6.4. In its CRM policies and procedures, a bank must consider whether, when calculating capital requirements, it is appropriate to give the full recognition of the value of the credit risk mitigant as permitted by the Instruction and must demonstrate that its CRM management policies and procedures are appropriate to the level of capital benefit that it is recognizing.

## 7. Credit Concentration Risk

- 7.1. A risk concentration refers to any single exposure or group of exposures that could result in losses large enough—relative to a bank's capital, total assets, or overall risk profile—to threaten the institution's financial soundness or its ability to maintain core operations. Risk concentrations are arguably the most significant contributors to major banking problems.
- 7.2. Risk concentrations can occur in a bank's assets, liabilities, or off-balance-sheet items, and may also emerge through the execution or processing of transactions (either product- or service-related), or through a combination of exposures across these categories. Given that lending is the primary activity of most banks, credit risk concentrations are typically the most material.
- 7.3. Credit risk concentrations are characterized by exposures sharing common or correlated risk factors, which, under stressed conditions, can negatively impact the creditworthiness of each individual counterparty within the concentration.

- 7.4. Concentration risk arises not only through direct exposures to obligors but also through exposures to credit risk protection providers. These types of concentrations are not explicitly addressed under the Pillar 1 capital charge for credit risk.
- 7.5. Banks must implement effective internal policies, systems, and controls to identify, measure, monitor, and manage their credit risk concentrations. Banks must comply with Instruction n° 2000/5, dated December 26, on Large Credit Exposures and Instruction n° 16/2021, of November 25, on Credit Risk Management when managing credit risk concentrations.
- 7.6. The extent of these concentrations should be explicitly considered in the bank's Pillar 2 capital adequacy assessment.
- 7.7. These policies should address the various types of credit risk concentrations to which a bank may be exposed, including:
- a) Significant exposures to an individual counterparty or a group of connected counterparties, referred to as large exposure limits. BCTL has imposed limits for such exposures in accordance with the above-mentioned Instruction 2000/5. Banks may also establish aggregate limits for managing and controlling all large exposures collectively.
  - b) Credit exposures to counterparties within the same economic sector or geographic region.
  - c) Credit exposures to counterparties whose financial condition depends on the same activity or commodity.
  - d) Indirect exposures arising from a bank's credit risk mitigation (CRM) activities (e.g., reliance on a single type of collateral or a single credit protection provider).
- 7.8. A bank's credit concentration risk management framework should be clearly documented. It should define what constitutes a credit risk concentration for the institution and outline how concentrations and corresponding limits are calculated. These limits should be expressed relative to the bank's capital, total assets, or - where appropriate - its overall risk profile.
- 7.9. Management should conduct regular stress tests on major credit risk concentrations and analyze the results to identify and address potential shifts in market conditions that could adversely affect the bank.

## **8. Counterparty Credit Risk (CCR)**

- 8.1. As counterparty credit risk (CCR) constitutes a form of credit risk, banks must adhere to the standards outlined in this framework regarding stress testing, residual risks associated with credit risk mitigation techniques, and credit concentrations, as discussed above.
- 8.2. Banks must maintain conceptually sound and integrity-driven policies, processes, and systems for managing CCR, aligned with the sophistication and complexity of the institution's exposures. A sound CCR framework must include the identification, measurement, management, approval, and internal reporting of such risk.
- 8.3. Risk management policies must account for market, liquidity, legal, and operational risks associated with CCR, and, to the extent feasible, the interrelationships among them. The bank must not enter into business with a counterparty without evaluating its creditworthiness, taking into account both pre-settlement and settlement risk. These risks should be managed comprehensively, both at the counterparty level (aggregating all exposures) and at the firm-wide level.
- 8.4. The board of directors and Senior Management must be actively engaged in CCR oversight and recognize it as a critical function requiring significant resource allocation. If the bank employs

an internal CCR model, Senior Management must be familiar with its assumptions, limitations, and how these affect reliability. They should also assess how market uncertainties (e.g., timing of collateral realization) and operational risks (e.g., pricing feed irregularities) are represented in the model.

- 8.5. Daily CCR exposure reports must be reviewed by Senior Management with sufficient authority to enforce position reductions at both the individual trader/credit manager level and the firm-wide level.
- 8.6. CCR management must operate in coordination with internal credit and trading limits. These limits should be clearly linked to the bank's risk measurement model and consistently applied and understood across business functions.
- 8.7. Banks must monitor daily and intra-day credit line usage. CCR measurement must capture current exposures, both gross and net of collateral, particularly for over-the-counter (OTC) derivatives and margin lending. A robust limit-monitoring system should also assess peak or potential future exposure at an appropriate confidence level, both at the portfolio and counterparty levels.
- 8.8. A rigorous CCR stress testing program must supplement model outputs. Test results should be reviewed by Senior Management and incorporated into CCR policies and limits. If vulnerabilities are identified, management should consider appropriate risk mitigation strategies, such as hedging or exposure reduction.
- 8.9. The bank must maintain compliance with a well-documented set of internal policies, controls, and procedures related to CCR system operation. The CCR management system must be documented (e.g., through a risk management manual) that describes its core principles and measurement techniques.
- 8.10. Banks must regularly conduct independent internal audits of the CCR management system. These audits should cover activities in both business and control units, and include a comprehensive review of the adequacy of system documentation, the organization of the collateral management unit, the organization of the CCR control unit, the integration of CCR into daily risk management, the approval process for pricing and valuation models, the validation of significant model changes, the scope of counterparty risk captured, the integrity of the management information system (MIS), the accuracy and completeness of CCR data, the reflection of legal terms in exposure calculations, the reliability and independence of data sources used for modeling, the validity of volatility and correlation assumptions, the accuracy of valuation and risk transformation methods, and frequent back testing of the model to verify accuracy.
- 8.11. Banks in Timor-Leste utilize the Standardized Approach to Counterparty Credit Risk (SA-CCR) to measure the required capital for CCR. Banks should regularly assess whether their implementation adequately captures CCR capital requirements.

## **9. Securitization**

- 9.1. A bank's on- and off-balance sheet securitization activities must be incorporated into its risk management processes, including product approval, risk concentration limits, and estimations of market, credit, and operational risks.
- 9.2. Given the broad range of risks arising from securitization - and the pace of innovation in related instruments - Pillar 1 capital requirements are often insufficient. Therefore, all securitization-related risks must be addressed within the bank's Internal Capital Adequacy Assessment Process (ICAAP). These include:
  - a) Credit, market, liquidity, and reputational risks of each exposure;
  - b) Potential delinquencies and losses on the underlying assets;

- c) Exposures from liquidity facilities or credit lines extended to special purpose entities (SPEs);
  - d) Exposures involving third-party guarantees.
- 9.3. Securitization exposures must be captured in the MIS, enabling Senior Management to understand their implications for liquidity, earnings, risk concentrations, and capital adequacy. Banks should maintain up-to-date information on securitization transactions, including market data, where available, and performance data provided by the trustee or servicer.
- 9.4. The complexity of a bank's monitoring system for early amortization events should be proportionate to the size and complexity of its securitization activities involving such provisions.

## **Article 15**

### **Liquidity Risk**

1. Banks must establish governance, policies, and systems for sound liquidity risk management.
2. Stress testing shall assess liquidity shortfalls under normal and stressed conditions, and contingency funding plans must be in place.
3. Liquidity stress testing shall also consider interactions between capital and liquidity, consistent with Basel III Liquidity Coverage Ratio (LCR) and Net Stable Funding Ratio (NSFR) standards.
4. A bank should both diligently manage its liquidity risk and maintain sufficient liquidity to withstand a range of stressful events.
5. Instruction n° 22/2023, dated July 04, on Liquidity Risk Management establishes the minimum standards for the sound management of liquidity risk. A bank is expected to thoroughly identify, measure, and control liquidity risks, particularly in relation to complex products and contingent commitments (both contractual and non-contractual).
6. This process should include the capability to project cash flows arising from assets, liabilities, and off-balance sheet items over various time horizons, while ensuring diversification in both the tenor and sources of funding. A bank should utilize early warning indicators to detect the emergence of heightened risk or vulnerabilities in its liquidity position or funding needs. It must be capable of managing liquidity risk exposure and funding requirements—across its organizational structure, legal entities, business lines, and currencies—while taking into account any legal, regulatory, and operational constraints on liquidity transferability.
7. A key element in liquidity risk management is strong governance, including the establishment of a liquidity risk tolerance by the board. This tolerance should be communicated across the institution and reflected in the strategies and policies set by Senior Management .
8. An additional aspect of liquidity risk management is the incorporation of the costs, benefits, and risks of liquidity into internal pricing, performance measurement, and new product approval processes across all significant business activities.
9. While banks typically manage liquidity under “normal” conditions, they must also be prepared to manage it under stressed scenarios. A bank should conduct regular stress tests or scenario analyses to identify and quantify its exposure to potential liquidity stresses, assessing their impacts on cash flows, liquidity positions, profitability, and solvency. These results should be thoroughly reviewed by management and should inform decisions to implement remedial or mitigating actions, such as building liquidity buffers or adjusting the bank's liquidity profile in line with its risk tolerance. Stress test results should also play a key role in contingency funding plans, which must clearly outline strategies for managing liquidity shortfalls under emergency conditions.

10. Senior Management should evaluate the interrelationship between liquidity and capital, as liquidity risk can affect capital adequacy and vice versa, potentially worsening a bank's liquidity profile.
11. Article 15 of Instruction n° 22/2023, of July 04, on Liquidity Risk Management requires banks to prepare an Internal Liquidity Adequacy Assessments (ILAA), in accordance with the guidelines established by BCTL, at least annually. Banks should consider the impact of such assessment on the capital requirements.

## **Article 16**

### **Strategic Risk**

1. Strategic risk emerges when a bank falters in executing suitable business plans, crafting effective strategies, making sound decisions, or allocating resources wisely. It also arises when the institution struggles to adapt to shifts in its external business landscape.
2. This type of risk, therefore, is closely tied to several key elements:
  - a) the strategic goals set by the institution,
  - b) the business strategies devised to attain these goals,
  - c) the resources committed to these efforts and the effectiveness of their deployment, and
  - d) the tangible and intangible assets required to execute these strategies.
3. These assets encompass communication systems, operational infrastructure, delivery networks, and the overall managerial expertise and capabilities of the institution. While directing strategic management, it becomes imperative to assess the institution's internal attributes against the backdrop of ongoing economic, technological, competitive, and regulatory changes.
4. Strategic risk may originate in numerous ways, but common sources within banking institutions include:
  - a) rising competition from new industry entrants;
  - b) disruptive shifts in technology;
  - c) evolving customer priorities and an overdependence on a limited client base;
  - d) economic volatility;
  - e) regulatory developments;
  - f) inefficiencies in work processes and procedures; and
  - g) inadequate information to support sound decision-making.
5. Each institution must establish a well-conceived strategic plan, grounded in a realistic and supportive budget. Such a plan articulates the institution's core purpose, sets forth its goals and priorities, and outlines pragmatic approaches for achieving them. However, if the strategic planning process is flawed - be it from unrealistic assumptions or inappropriate methodologies - the institution may find itself vulnerable to strategic risk.
6. To prevent this, institutions should ensure their strategic planning process encompasses:
  - a) active involvement from the Board, its delegated committees, and senior leadership,
  - b) contributions from personnel across various departments,
  - c) sufficient information to build credible assumptions related to economic dynamics, market standing, competition, future trends, and customer expectations,
  - d) alignment between operational initiatives and the institution's overarching goals, and

- e) regular evaluation of actual performance against strategic objectives.
- 
- 7. In pursuit of strategic resilience, institutions must implement comprehensive and effective risk mitigation frameworks. This involves recruiting a competent Board and executive team, developing strategic and operational plans, maintaining a skilled and well-trained workforce, instituting robust risk management systems, and ensuring broad access to timely and relevant information.
  - 8. Managing strategic risk effectively demands the formulation of sound policies, procedures, and limits—approved by the Board—that allow for clear evaluation and responsiveness to the changing business environment.
  - 9. Policies on strategy should provide direction on which business segments to prioritize, both in the short and long term. They must address all significant risks tied to these segments, as outlined in the strategic plan. Clear lines of accountability and authority must be established throughout the organization.
  - 10. These policies must align with the institution’s broader goals, capital adequacy, technical capacity, and risk appetite. They should take into account the institution’s size, complexity, and past experiences, ensuring that any strategic reevaluation considers:
    - a) the institution’s core strengths,
    - b) its recognized weaknesses,
    - c) opportunities available in the external environment, and
    - d) potential threats arising from outside forces.
  - 11. Strategic risk policies should incorporate risk mitigation tools and techniques, including a set of limits to manage exposure to measurable risks associated with the strategic plan. At a minimum, these limits should cover exposure levels to different economic sectors, targeted business growth and staffing plans, and expansion of the institution’s operational network.
  - 12. Banks must assess the strategic risk and set a minimum capital to face the risk under Pillar II. The Board of Directors and Senior Management should examine a bank’s current and future capital requirements in relation to its strategic business objectives, determine the bank’s near- and longer-term capital needs, the capital expenditures required for the foreseeable future, the target capital levels, and external capital sources.

## **Article 17**

### **Reputational Risk**

- 1. Reputational risk emerges not merely from events, but from the perceptions they create and are held by customers, counterparties, investors, regulators, analysts, and the broader public. These impressions, whether grounded in fact or driven by sentiment, can undermine a bank’s ability to maintain long-standing relationships or foster new ones. Most critically, they may constrain access to funding, especially in confidence-sensitive environments like the interbank market. Reputational risk, therefore, is not one-dimensional; it is shaped by the collective lens through which the institution is viewed by the financial ecosystem.
- 2. At its core, a bank’s exposure to reputational harm is intimately tied to the strength of its internal risk controls and the agility of its leadership in responding to events that touch its operations or public image. A mishandled reputational event can push an institution into making unplanned commitments (as supporting entities or products beyond its legal obligations) only to find itself entangled in deeper credit, market, legal, or liquidity risks. The ripple effects of such actions can be profound, striking at the heart of the bank’s earnings, capital, and liquidity reserves.

3. A vigilant institution does not wait for perception to shift before acting. Instead, it takes a proactive stance—identifying where reputational vulnerabilities may lie. These may arise from routine operations, complex liability structures, affiliated entities, off-balance sheet exposures, or the specific markets in which the bank operates. Embedding these concerns into comprehensive risk management frameworks, including ICAAP and contingency planning for liquidity, is not optional; it is essential.
4. Reputational harm often carries direct consequences for a bank's liabilities. Market confidence is fragile, and a tarnished reputation can disrupt funding lines, narrow financing options, and amplify liquidity strain. In a bid to restore trust, banks may feel compelled to honor obligations ahead of schedule or take actions that, while preserving reputation, can compromise short-term liquidity.
5. It is incumbent upon management to establish clear, forward-looking policies for identifying and measuring reputational risk. These policies should be particularly attentive when the bank ventures into new markets, launches unfamiliar products, or undertakes non-traditional lines of business. Reputational concerns should also be included into stress testing, helping management anticipate not only immediate consequences but also the cascading effects that reputational damage can trigger across other domains.
6. When potential exposure is identified, the bank must gauge the extent of support it might be expected to offer, or the losses it may have to absorb, especially in times of market stress. Quantitative and qualitative methods should be enhanced to reflect the true weight of reputational events, and their potential to amplify credit, market, liquidity, or operational risks. Embedding reputational scenarios into stress-testing exercises is one way to bring this clarity.
7. Lastly, particular vigilance is needed regarding reputational shocks and their implications for liquidity. A damaged reputation can create simultaneous demands: the need to step in and support faltering structures, and the challenge of diminished market trust, which may cut off vital funding channels. Navigating these dual pressures requires foresight, discipline, and a firm commitment to preserving both credibility and resilience in an increasingly scrutinized financial landscape.
8. Banks must integrate reputational considerations into ongoing assessments of credit, market, legal, or liquidity risks and ensure that adequate capital is constituted to absorb the impact of the reputational risk.

## **Article 18**

### **Market Risk**

1. Instruction 21/2023, of July 04, on Regulatory Capital and Leverage sets clear policies and procedures to determine which exposures may be included in (or must be excluded from) the trading book for regulatory capital calculation.
2. Such policies must clearly define the boundaries of the trading book and must align with the bank's risk management capabilities and practices.
3. Transfers between the banking book and trading book should only occur under limited and permitted circumstances.
4. Instruments held in the trading book must be governed by clearly defined policies and procedures, approved by Senior Management , to ensure active risk management. These must be thoroughly documented and should, at a minimum, address the following:
  - a) The activities considered trading or hedging of covered instruments;
  - b) Trading strategies (including the expected holding period and actions if limits are breached) for each covered instrument or portfolio;

- c) Standards for daily mark-to-market of covered instruments, referencing an active, liquid two-way market;
- d) For instruments marked-to-model, standards for:
  - i. Identifying material risks;
  - ii. Hedging material risks and evaluating the liquidity of hedging instruments;
  - iii. Estimating key assumptions and parameters reliably;
- e) Requirements for externally validated valuations;
- f) Consideration of operational impediments to immediate liquidation;
- g) Active management processes, including:
  - 1) Setting and monitoring limits;
  - 2) Documented trading strategies and processes for compliance monitoring;
  - 3) Evaluation of stale positions and turnover;
  - 4) Autonomy of traders within approved limits;
  - 5) Reporting mechanisms to Senior Management ;
  - 6) Ongoing monitoring using market information, such as:
    - i. Market liquidity and hedging capability;
    - ii. Market value sensitivities to risk factors;
    - iii. Quality and availability of market inputs, turnover levels, and instrument size.
- 5. The bank must adopt a consistent methodology to identify and quantify banking book risks to be hedged through internal transfers. This methodology must be integrated into the bank's risk management framework and comply with all qualitative and quantitative regulatory requirements applicable to trading desks. Material changes must be approved by the Risk Management Committee or a designated committee.
- 6. A bank must have robust internal controls and risk management methods to ensure the effectiveness of internal risk mitigation. These methods must reflect the scope, nature, and complexity of such activities and be reviewed regularly.
- 7. Prudent valuation policies are the cornerstone of sound market risk capital adequacy. For a diversified portfolio of highly liquid cash instruments with no market concentration, standard valuation practices and quantitative requirements may suffice. However, for portfolios that are less diversified, less liquid, concentrated, or heavily reliant on mark-to-model, additional capital may be necessary to account for valuation uncertainty. Where capital shortfalls are identified, the bank must reduce risk and/or increase capital holdings accordingly.

## **Article 19**

### **Interest Rate Risk (in banking book)**

1. Interest rate risk (in banking books) refers to the potential impact of adverse movements in interest rates on a banking institution's financial condition. While managing interest rate risk is an inherent and often profitable aspect of banking, excessive exposure can threaten earnings and capital stability.
2. Changes in interest rates influence a bank's performance by altering the net interest income and other interest-sensitive revenues and expenses or the economic value of assets, liabilities, and off-balance sheet (OBS) items, due to shifts in the present value of expected future cash flows.

3. An effective risk management framework is essential to maintain interest rate risk at prudent levels, thereby safeguarding the bank's financial health.
4. The key types of interest rate risk comprise:
  - a) Repricing Risk. The most common form of IRR, repricing risk arises when assets, liabilities, or OBS instruments reprice at different times or to different extents. This mismatch is a core feature of banking, often stemming from funding long-term assets with short-term liabilities or vice versa.
    - i. Liability-sensitive institutions (liabilities reprice faster): earnings tend to increase when rates fall and decrease when rates rise.
    - ii. Asset-sensitive institutions (assets reprice faster): benefit from rising interest rates but are adversely affected by falling rates.
  - b) Yield Curve Risk. The yield curve risk occurs when interest rates change unevenly across various maturities. Even if assets and liabilities are linked to similar benchmarks, differences in their maturity profiles can lead to gains or losses when the yield curve steepens, flattens, or inverts.
  - c) 3) Basis Risk. This arises when assets and liabilities are priced using different market indices that do not move in perfect correlation. Basis risk also includes mismatches in hedge and exposure durations, leading to imperfect risk coverage.
  - d) Optionality Risk, which originates from embedded or explicit options in financial instruments that can alter cash flows based on interest rate changes. Examples include:
    - i. Callable bonds or notes
    - ii. Prepayable loans (e.g., residential mortgages)
    - iii. Non-maturity deposits (e.g., demand deposits) where customers can withdraw funds at will
  - e) Price Risk, which refers to changes in the fair value of financial instruments—such as trading portfolios, loans held for sale, or mortgage servicing rights—as interest rates fluctuate.
5. Interest rate risk can adversely affect both earnings and capital:
  - a) Earnings Impact: Most institutions focus on net interest income, the difference between interest earned and interest paid. However, interest rates also impact non-interest income (e.g., loan servicing fees or securitization income), especially in institutions where these revenues are substantial. Risk measurement systems should account for both net interest income and total net income.
  - b) Capital Impact (Economic Value of Equity): Interest rate changes affect the present value of assets and liabilities, thereby impacting the institution's equity. Management should assess how shifts in rates influence long-term value through changes in the economic value of equity (EVE). For example, in a rising rate environment, fixed-rate bond values typically decline.
6. Though few banks have failed solely due to interest rate movements, improper interest rate risk management can significantly undermine profitability, especially in today's fast-evolving financial landscape. A sound interest rate risk management process should:
  - a) Monitor repricing and duration gaps
  - b) Measure exposure using net interest income and economic value of equity approaches
  - c) Include stress testing and scenario analysis
  - d) Adapt to changing market conditions and financial innovations.

**Article 20**  
**Operational Risk**

1. Operational risk is the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.
2. Operational risk event types having the potential to result in substantial losses include:
  - a) Internal fraud. For example, intentional misreporting of positions, employee theft, and insider trading on an employee's own account.
  - b) External fraud. For example, robbery, forgery, cheque kiting, and damage from computer hacking.
  - c) Employment practices and workplace safety. For example, workers compensation claims, violation of employee health and safety rules, organized labor activities, discrimination claims, and general liability.
  - d) Clients, products and business practices. For example, fiduciary breaches, misuse of confidential customer information, improper trading activities on the banking institution's account, money laundering, and sale of unauthorized products.
  - e) Damage to physical assets. For example, terrorism, vandalism, earthquakes, fires and floods.
  - f) Business disruption and system failures. For example, hardware and software failures, telecommunication problems, and utility outages.
  - g) Execution, delivery and process management. For example, data entry errors, collateral management failures, incomplete legal documentation, unapproved access given to client accounts, non-client counterparty mis performance, and vendor disputes.
3. Instruction 21/2023 dated July 04, on Regulatory Capital and Leverage sets the minimum capital required for Operational Risk. However, the measure adopted is one of more simplified models for measuring the risk. A bank should consider a measurement of Operational Risk consistent with its size and operations and determine if the basic indicator model is adequate. If the bank considers that the model cannot capture all the operational risks involved in its operation, the bank should determine the additional capital required for operational risk.

**SECTION IV**  
**CAPITAL ADEQUACY ASSESSMENT**

**Article 21**  
**Sound Capital Adequacy**

1. Banks must conduct comprehensive capital adequacy assessments over a planning horizon of at least three years, ensuring alignment between business strategies, capital needs, and supervisory requirements.
2. A thorough analysis of a bank's current and future capital needs in alignment with its strategic objectives is a critical component of the bank's strategic planning process. The strategic plan should clearly articulate capital requirements, expected capital expenditures, target capital levels, and potential sources of external capital.
3. Banks bear the responsibility for ensuring that their internal capital assessments are both comprehensive and appropriate to the nature and complexity of the risks arising from their business activities and operating environment.
4. Fundamental elements of sound capital assessment include:

- a) A clearly defined and documented process for evaluating risks and determining whether these risks necessitate holding specific amounts of capital.
  - b) Policies and procedures that ensure the identification, measurement, and reporting of all material risks;
  - c) A process that relates current and projected capital levels to the bank's risk profile, in line with the Board of Directors' approved risk tolerance;
  - d) A framework for setting capital adequacy objectives in relation to risk, considering the bank's strategic direction and business plan;
  - e) Internal controls, review mechanisms, and audit processes to uphold the integrity of the overall capital management framework.
5. Banks must also maintain an effective capital planning process, which includes:
- a) Assessing both the risks they face and the adequacy of their risk management frameworks;
  - b) Implementing processes to manage and mitigate identified risks;
  - c) Evaluating capital adequacy relative to their overall risk exposures;
  - d) Considering the potential impacts of economic downturns on earnings, liquidity, and capital levels.
6. Banks must define the time horizon over which capital adequacy is assessed, being the minimum of three years forward, and ensure alignment between long-term capital targets and short-term objectives.
7. The capital planning process should account for the potential lead times and costs associated with raising additional capital, particularly under stressed market conditions. Accordingly, banks should consider the challenges of accessing capital during downturns or periods of financial strain.

## **Article 21**

### **ICAAP Reporting and Review Process**

1. On an annual basis, bank shall submit to BCTL the ICAAP report approved by Board of Directors, in accordance with Article 9, Paragraph 3 of the Instruction 24/2023, on Reporting and Publication.
2. Banks must reconcile differences between accounting capital (as reported under IFRS) and regulatory capital (as defined under Basel III), ensuring transparent adjustments between IFRS equity and Common Equity Tier 1 (CET1). Such reconciliation should be documented within the ICAAP report.
3. ICAAP reports shall explicitly demonstrate compliance with Basel III capital ratios, buffers, leverage ratio, LCR, and NSFR, and explain how IFRS 9 provisioning methodologies are embedded in the forward-looking capital assessment.
4. Banks can prepare the ICAAP in accordance with the methodology that best suits their needs but should consider all elements referred to in these Guidelines. The report should have descriptive and analytical elements.
5. Annex I to the Guidelines is a template with a suggested structure for the presentation of the ICAAP Report. Banks are not obliged to follow the template. Independently of the format, the ICAAP report shall contain an executive summary, a description of the business model and strategic initiatives, a summary of financial indicators, details of the governance structure, definition of the risk profile in terms qualitative and quantitative, analysis of the risks under Pillar I and Pillar II, assessment of capital requirements and capital resources, summary of capital projections for next three years, impact of stress testing, integration of ICAAP to risk management, documentation, reporting and review.

6. Banks must be able to demonstrate to the BCTL that the chosen internal capital target levels are well founded and that these targets are consistent with their overall risk profile and current operating environment
7. Banks do not need to submit the documents used for the preparation of the ICAAP Report to the BCTL. However, such documents should be kept available at the banks' headquarters for evaluation by the BCTL.
8. BCTL may require banks to submit ICAAP outcomes more than once a year if necessary for adequate supervision.
9. BCTL has the ability to review the submitted ICAAP using the methods available:
  - a) off-site analysis.
  - b) on-site reviews; and
  - c) discussions with the bank.
10. BCTL can require adjustments to the level of Capital Adequacy as a consequence of the ICAAP Report and its supervisory assessment, according to Regulation 2000/8 on Banking Licensing and Supervision or Instruction 21/2023 on Regulatory Capital and Leverage.

## Annex I: Template for the ICAAP Report

### 1. Executive Summary

**Purpose:** Summarize the ICAAP's objectives, scope, and key findings.

- **Capital Adequacy Assessment:** The institution has assessed its capital as adequate on a consolidated basis, considering the size and complexity of its operations.
- **Material Risks Overview:** Key risks identified include credit, market, operational, liquidity, interest rate, concentration, strategic, and reputational risks. The institution has evaluated the acceptability of these risks and outlined mitigation plans where necessary.
- **ICAAP Findings:**
  - Determination of internal capital levels and composition relative to the institution's risk profile. and compared to regulatory requirements under Pillar 1.
  - Assessment of risk management processes' adequacy.
  - Integration of financial, strategic, and capital planning with risk management and decision-making processes.
  - Evaluation of capital resources' adequacy over the planning horizon.
  - Establishment of target capital metrics, including Common Equity Tier 1 (CET1) Ratio, Tier 1 Ratio, Total Capital Ratio, and Leverage Ratio.
  - Summary of stress test results and their implications for capital management.
- **Financial Position and Strategy:** A concise overview of the institution's financial standing, business strategy, balance sheet structure, and projected profitability.
- **Governance:** Description of the ICAAP's review, challenge, and approval processes, emphasizing board involvement.

### 2. Background of ICAAP

- **Integration with Risk Management:** Explanation of how the ICAAP aligns with the institution's risk management framework, strategy, business planning, and capital management.
- **Policies and Systems:** Overview of policies and systems used to identify, manage, and monitor risks in accordance with the institution's risk appetite.
- **Business Model:** Description of core activities, markets served, and strategic direction.
- **Financial Position:** Analysis of current financial standing, including capital structure and profitability.
- **Strategic Initiatives:** Outline of planned business developments and their potential impact on risk profile and capital needs.
- **Governance Structure:** Details of the roles and responsibilities of the Board, Senior Management, and risk committees in overseeing ICAAP.
- **Internal Controls:** Overview of policies, procedures, and systems in place to identify, measure, monitor, and control risk

### 3. Statement of Risk Appetite

- **Risk Appetite Framework:** High-level overview of the institution's risk appetite, including definitions of risk tolerance levels and the frequency of reviews by management and the board.

#### 4. **Material Risks**

- **Risk Identification Process:** Description of the processes used to identify material risk areas.
- **Key Risks Considered:**
  - Credit Risk
  - Market Risk
  - Operational Risk
  - Interest Rate Risk (in the Banking Book)
  - Concentration Risk
  - Funding and Liquidity Risk
  - Business/Strategic Risk
  - Reputation Risk
  - Residual Risk

#### 5. **Capital Planning**

- **Baseline Capital Forecasts:** Quarterly forecasts based on the annual business plan.
- **Three-Year Capital Projections:** Summary of projected capital positions and main assumptions.
- **Capital Requirements:** Calculation of capital needs for each material risk, considering both Pillar 1 and Pillar 2 requirements.
- **Capital Resources:** Inventory of available capital, including Common Equity Tier 1 (CET1), Additional Tier 1 (AT1), and Tier 2 capital.
- **Capital Buffers:** Assessment of capital buffers in place to absorb losses during periods of stress.
- **Leverage Ratio:** Assessment of the leverage ratio and any capital requirement.
- **Internal Capital Targets:** Establishment of internal capital targets above regulatory minima to ensure resilience.
- **Capital Planning Process:** Description of how the ICAAP is incorporated into capital planning and management processes.

#### 6. **Stress and Scenario Testing**

- **Stress Testing Program:** Overview of the stress testing program used to support capital adequacy assessment and management.
- **Scenario Development:** Development of institution-specific, forward-looking scenarios aligned with the business model and risk profile.
- **Management Actions:** Articulation of potential management actions in response to stress scenarios, including feasibility assessments and implementation timeframes.

#### 7. **Integration of ICAAP into Risk Management**

- **Decision-Making Processes:** Explanation of how ICAAP results are embedded in decision-making processes.
- **Risk Limits Setting and Monitoring:** Description of how ICAAP outcomes influence risk limits and monitoring.
- **Board Reporting:** Details on how ICAAP results are communicated to the board and approved.

- **Third-Party Review:** Identification of any external reviews conducted on the ICAAP.
- **Enhancement Plans:** Plans for future enhancements to the ICAAP.