Republic of Panama
Superintendency of Banks

RULE N°. 11-2018[1]
(dated 11 September 2018)

"Whereby new provisions on Operational Risk are prescribed"

THE BOARD OF DIRECTORS
in use of its legal powers and,

WHEREAS:

Due to the issuance of Decree Law 2 dated 22 February 2008, the Executive Branch re-edited Decree Law 9 dated 26 February 1998 and all its amendments as a consolidated text, and this text was approved by means of Executive Decree 52 dated 30 April 2008, hereinafter referred to as the Banking Law;

Pursuant to the provisions of paragraphs 1 and 2 of Article 5 of the Banking Law, safeguarding the soundness and efficiency of the banking system and strengthening and fostering favorable conditions for the development of the Republic of Panama as an international financial center are objectives of the Superintendency of Banks;

According to the provisions of paragraphs 3 and 5 of Article 11 of the Banking Law, approving general criteria for the classification of assets at risk and rules for the provision of reserves against risk and establishing the administrative interpretation and scope of the legal provisions and regulations on banking matters are among the technical duties of the Board of Directors;

In accordance with Article 6 of the Banking Law, ensuring that banks maintain sufficient liquidity and solvency ratios to discharge their obligations is one of the duties of the Superintendency of Banks;

Pursuant to the provisions of Article 72 of the Banking Law, the Superintendency may take into account the presence of other risks that may serve to evaluate the need for capital funds, including market risk, operating risk, and country risk in determining the capital adequacy ratios;

The Basel Committee on Banking Supervision's Core Principles for Effective Banking Supervision establishes that banks must have a comprehensive risk management process, including oversight by the board of directors and top management, to identify, quantify, assess, oversee, report and control or mitigate all substantial risks in a timely manner, as well as to assess capital and liquidity sufficiency associated with the risk profile;

Given the evolution of the prudential regulations, best banking practices and accounting and auditing standards, it is necessary to update the general regulatory framework governing the International Banking Center;

Banks, according to their features, operations and the products they offer, take operational risks. Consequently, they must assess this risk as part of their risk management process;

By means of Rule 7-2011 dated 20 December 2011 Operational Risk rules were prescribed;

During its working sessions, the Board of Directors determined it was necessary and advisable to update the provisions on operational risk management pursuant to international standards

RESOLVES:

[1] Amended by Rule 3-2019 dated 30 April 2019.

OPERATIONAL RISK MANAGEMENT STANDARD

CHAPTER I
GENERAL PROVISIONS

ARTICLE 1. OBJECTIVE AND CRITERIA. This Rule establishes the principles, general criteria and minimum requirements that all banks must meet when designing, developing and implementing their operational risk management system, which must include the identification, measurement, mitigation, monitoring and control, and reporting of operational risks.

ARTICLE 2. SCOPE OF APPLICATION. The provisions in this Rule are applicable to banks, as provided for in Article 1 of the Rule on Capital Adequacy issued by the Superintendency.

Notwithstanding the above, the aspects related to operating risk management covered in this Rule will only be applicable to general license banks and international license banks whose home supervisor is the Superintendency of Banks.

International license banks whose host supervisor is the Superintendency of Banks must establish their own internal mechanisms for an appropriate operational risk management that will be subject to the Superintendency's review. However, the Superintendent may insist that local management, when he deems it appropriate, follow the requirements of operational risk management provided in this Rule.

ARTICLE 3. TERMS AND DEFINITIONS. In order to apply the provisions in this Rule, the following terms will be understood as follows:

1. **Board of Directors:** The body responsible for the direction and control of the bank, which ensures the achievement of the best interests of the entity without getting involved in the direct management of the bank's business.

2. **Top Management or Senior Management:** The highest executive authority (namely: General Manager, Executive Vice President, Chief Executive Officer or other title) as well as the second highest-raking executive (namely: Deputy General Manager or other title) and the other managers and employees discharging key duties who must directly report to the aforementioned.

3. **Comprehensive Risk Management:** The process whereby the bank identifies, measures, monitors, controls, mitigates and reports the different type of risks to which the bank is exposed.

4. **Operational risk:** The possibility of incurring in losses due to deficiencies, failures or unfitness of human resources, processes, technology, infrastructure, information management, models used, or external events. This definition includes the legal risks related to such factors, but excludes business interruption, reputational risk and strategic risk.

5. **Legal risk:** The possibility of incurring in losses from a breach of standards, laws, regulations, or procedures with potential legal consequences, as well as of instructions issued by law enforcement entities, negative judicial or administrative resolutions, in- or out-of-court agreements, arbitration awards, as well as the poor wording of texts, affecting the implementation, formalization or execution of acts, agreements or transactions, including those not part of the ordinary course of business, or because the rights and duties of the contracting parties have not been properly stipulated.

6. **Operational risk event:** An internal or external event that causes or could cause losses to the bank.

7. **Operational risk incident:** An internal or external event that causes losses to the bank.

8. **Operational risk categories:** The factors in which operational risk is classified, depending on the nature of the threat.

9. **Process:** The set of activities that transforms raw materials into products or services with value to an internal or external end-user.

10. **Business line:** A business specialization that groups processes aimed at producing specialized products and services to serve a segment of the target market.

11. **Operational risk appetite:** The level of operational risk the entity is willing to take. Determining the appetite for risk is part of developing the risk management systems. It is established by means of risk parameters and indicators.

12. **Risk tolerance:** The highest deviation the bank can handle with regard to the established appetite for risk.

13. **Risk limits:** The highest deviation permitted with regard to the values established for risk tolerance.

14. **Risk appetite framework:** An overall system including the information policies, organization, processes, controls and systems by means of which the entity's risk is managed. It should include the indicators that permit defining the appetite for risk, tolerance levels and risk limits.

15. **Risk profile:** It is defined from assessing the quantity and magnitude of residual risk exposures to the bank's business and administrative activities.

16. **Identified operational risks:** Internal or external threats that, if made true, may cause accounting losses to the entity.

17. **Frequency:** The number of times an event or incident occurs.

18. **Exposure:** The amount of the potential highest loss for the occurrence of an operational risk event or incident, without taking into consideration the decrease from coverages or recoveries.

19. **Severity:** Difference between exposure and amount recovered by coverages and others.

20. **Inherent risk:** The risk inherent in any process or activity, taking into consideration the frequency and the impact, before controlling it.

21. **Residual risk:** The result of assessing the risks inherent in the activity or process, after applying the relevant controls to reduce the probability that identified operational risks occur.

22. **Global limit:** The highest amount of operational risk the bank can endure, distributed in ranges according to the criticality level the entity has set.

23. **Criticality level:** The level of risk with which the frequency, exposure and severity of events and incidents are assessed pursuant to the established limits.

24. **Specific limits:** The global limit component assigned to each type of operational risk, distributed in ranges according to the criticality levels the entity has set.

25. **Risk map:** The graphic representation of the operational risk exposure by risk type, contents of the risk matrices and databases.

26. **Operational risk database:** A repository where the operational risk events or incidents are registered, with a sufficient description and necessary historical depth that contribute to the management of these risks.

27. **Operational Risk Indicators (ORI):** A form of measurement aimed at providing an early warning on the behavior of operational risks that occurred.

28. **Mitigation:** The reduction of exposure to major operational risks, making the controls more robust or using programs or risk coverage as complements to internal control measures.

CHAPTER II
APPROPRIATE ENVIRONMENT FOR OPERATIONAL RISK MANAGEMENT

ARTICLE 4. ORGANIZATION. Banks must have an organizational structure that is fitted to the sophistication of their operations and risk profile. They must have an organizational structure that fosters an adequate operational risk management. They must also clearly define the responsibilities and the degree of dependence and interrelationship between the different areas of the bank.

As set forth in the Rule on Comprehensive Risk Management, the organizational structure must have an independent Risk Management Unit. This unit must have operational risk management as one of its duties.

At the same time, the Risk Committee must oversee operational risk management.

ARTICLE 5. MANAGEMENT STRATEGY. Banks must develop a strategy for operational risk management. Thus, it is important that the strategy define or identify the appropriate resources in trained staff, processes, information systems and the entire environment necessary for operational risk management.

To achieve that, the bank must establish a methodology that will allow for the identification, measurement, mitigation, monitoring, control, and reporting of this risk.

Considering that potential market changes affect the bank's economic and operational environment, and, furthermore, that all areas of the financial entity produce potential operational risks, the strategy and therefore the methodology must be reviewed on an annual basis, and must have the approval and support of the Board of Directors.

Top management must establish the procedures that ensure an appropriate flow, quality and opportunity of the information among the business units and all the persons involved in the operations implying risks for the bank.

ARTICLE 6. POLICIES. Banks must develop operational risk policies, manuals and procedures, including, as a minimum:

1. The duties and responsibilities of the board of directors, top management, the risk committee, and the risk management unit;

2. A detailed description of the operational risk process management (i.e. identification, measurement, mitigation, monitoring, control and reporting);

3. A description of the measurement tools, including:

    a. The operational risk profile;

    b. Operational risk matrices;

    c. Global limits and specific limits;

    d. Operational Risk Indicators (ORI);

    e. Maps of inherent and residual risk by type of risk;

    f. Operational risk database.

4. The process that must be followed, among other aspects, for the approval of new operations, products and services;

5. The form and frequency in which the results of the operational risk management must be reported to the board of directors, the risk committee and top management.

CHAPTER III
OPERATIONAL RISK MANAGEMENT

ARTICLE 7. OPERATIONAL RISK FACTORS OR CATEGORIES. Banks must consider the following operational risk factors:

1. **Human resources.** Banks must manage human resources in an appropriate manner and adequately identify the mistakes or inadequacies associated with the "human" factor, such as: lack of trained staff, negligence, human error, sabotage, fraud, robbery, misappropriation of sensitive information, nepotism, inappropriate interpersonal relationships, unfavorable working environment, and a lack of clear specifications in staff contracts, among others.

2. **Internal processes.** For the purpose of ensuring the optimization of resources and the standardization of activities, banks must have well-documented, defined and continuously updated processes.

   Banks must adequately manage the risk associated with operations and service procedures, as their inappropriate design could result in a deficient development of operations.

3. **Technology.** Banks must have the information technology that ensures capturing, processing, storing and reporting information in a timely and reliable manner that prevents business interruption and ensures that all information, including information provided through third party services, is complete, confidential and available for appropriate decision-making.

   In addition, banks must meet the requirements established in the regulations regarding this matter issued by the Superintendency of Banks.

4. **External threats.** Banks must manage the risk of losses from the occurrence of events which are beyond the control of the institution but that may affect their activities. They must take into account the risk of legal contingencies, the failure of public services, natural disasters, attacks and criminal activities, and failures in services provided by third parties.

5. **Information management.** All the bank's decisions are based on hypotheses, data, reports and analyses exposed to mistakes, from the analysis of the competitive environment, market analysis in which the entity is involved, the information collected for risk decisions and the degree of customer satisfaction, to the specific information systems to assess the entity's liquidity, solvency and profitability. The bank must frequently review the accuracy of the hypotheses, data, reports and analyses it uses and dedicate resources to improve them, both [in terms of] the entity's external reality and its own reality.

6. **Model risk.** Using models, especially for valuating financial instrument market value, designing rating systems, estimating loan loss provisions based on expected losses and, in general, measuring the different risk types, is a relevant source of operational risk. The contrast of the models must be an integral part of the operational risk management.

ARTICLE 8. MANAGEMENT. The operational risk management process consists of identifying, measuring, mitigating, monitoring and controlling, and reporting operational risk events.

ARTICLE 9. IDENTIFICATION. As part of operational risk management, the risk management unit and the owner of the process must identify threats that are inherent in their processes, products, services, and/or business areas and administration that may cause losses, grouping them as follows:

1. **Internal fraud.** Potential losses incurred by bank employee fraud, misappropriation of property or failure to comply with regulations, laws or internal policies;

2. **External fraud.** Potential losses incurred by third party fraud, misappropriation of property or failure to comply with legislation;

3. **Labor relationships and safety on the job.** Potential losses from acts incompatible with legislation or labor agreements, with safety and hygiene in the workplace, with payments of personal injury claims or with cases of discrimination or breaches of the code of ethics;

4. **Practices related to clients, products and business.** Potential losses caused by failure to comply with an obligation to clients or derived from the nature or design of a product or service. Also considered as practices related to clients are the betrayal of trust, the abuse of a client's confidential information, fraudulent negotiation in bank accounts, money laundering and the sale of unauthorized products;

5. **Damage to property.** Potential losses derived from damages to material assets as a result of natural disasters or other events;

6. **Business interruption due to information technology failure.** Potential losses from business interruption and technology systems failure;

7. **Deficiency in the execution, delivery or management of processes.** Potential losses from errors in processing operations or managing processes, as well as relationships with counterparties (suppliers, clients, depositors, etc.).

8. **Deficiency of a legal nature.** Potential losses due to penalties imposed for breaching laws and regulations, as well as a consequence of lawsuits against the bank, and for design flaws or execution of contracts related to the various financial instruments.

9. **Deficiency in management reporting systems.** Potential losses due to discrepancies between the analyses supporting decision-making and the underlying reality.

10. **Deficiency in models.** Potential losses resulting from the unsuitability of certain models when valuating financial instruments and the identification and measurement of risks, originating from inappropriate hypotheses, biased estimates of certain parameters, failure to include relevant variables, mistakes in databases used and even model manipulation.

The operational risks identified by the entity in its processes, products, services, service and support areas, management and models will be documented in operational risk matrices that must contain as a minimum:

1. The process or activity;
2. Description of the identified risk;
3. Type of risk;
4. Cause;
5. Assessment of periodicity and impact
6. Assessment of inherent risk
7. Control description
8. Quantitative control assessment
9. Residual risk assessment

The matrix or matrices must be reviewed on an annual basis pursuant to changes in the processes, business activities and support or the behavior of operational risks.

ARTICLE 10. MEASUREMENT. As part of operational risk management, the bank must continuously evaluate operational risk events and incidents using the following tools:

1. Risk profile;
2. Risk mapping;
3. Global limit and specific limits;
4. Operational Risk Indicators (IRO);
5. Operational risk databases

This implies, as a minimum:

1. Measuring exposures (frequency and impact) and losses by type of risk and their comparison with the global limit and specific limits set by the entity;

2. Measuring and analyzing the historical behavior of operational risks to establish and implement corrective actions to strengthen internal control when exposure increases or

there are losses incurred between surveyed periods, or when deviations from established limits occur.

Whenever possible, estimate the probability of the operational risk events, including the level of trust in these estimations, to establish greater mitigation or coverage measures, if necessary.

ARTICLE 11. MITIGATION. As part of operational risk management, once the threats and failures or vulnerabilities that have occurred in the entity have been identified, the risk committee and top management must decide whether the risk must be taken, shared, avoided or transferred, reducing its consequences and effects, to have a clear view of the different types of exposures to operational risk and their priority, aimed at establishing an action plan to increase measures to mitigate these risks.

This plan must describe the following, as a minimum:

1. Risk description;
2. Actions to be implemented;
3. Administrative unit responsible for its execution;
4. The measure's approval date;
5. Estimated date of execution;
6. Actual implementation date.

The effectiveness of the mitigation plan and action will be evaluated by the bank through the operational risk monitoring tasks.

ARTICLE 12. MONITORING AND CONTROL. As part of operational risk management, the bank must conduct monitoring to ensure that all actions implemented to mitigate an (identified or occurred) risk are met within the established period and that these measures have effectively contributed to reducing the possibility that similar events could occur in the future.

Monitoring tasks must be documented and conducted according to the strategy defined by the bank in a period no longer than one year.

ARTICLE 13. REPORTING. As part of operational risk management, the bank must ensure that the risk committee, top management and the Board of Directors are informed in a timely manner on the results of the operational risk management conducted and the level of operational risk to which the bank is exposed.

To this end, the risk management unit must include the following, as a minimum, in its reports:

1. The bank's risk exposure by type of risk and the result of comparing it to the global limit and specific limits;

2. The historical behavior of the exposures and losses taken;

3. The suggestions on the corrective actions that can be implemented as a result of a deviation in the established limits;

4. The results of the capital requirements for operational risk and historical behavior;

5. The behavior of operational and legal risk indicators;

6. The result of the monitoring tasks to ensure that all actions are implemented.

This stage also includes [the requirement for] operational areas to periodically receive information on events and incidents in order to take the necessary actions regarding them.

ARTICLE 14. METHODOLOGY. Banks shall establish a methodology based on their risk profile and the sophistication of their operations that will include all operational risk management stages (identification, measurement, mitigation, monitoring, control and reporting) and comply with the following requirements:

1. Be fully documented;

2. Be implemented in all bank areas;

3. Allow for the continuous improvement of operational risk management, which must be updated at least once a year;

4. Be integrated with all of the risk management processes of the entity;

5. Establish procedures that ensure compliance;

6. Be reviewed by the risk committee and approved by the board of directors.

ARTICLE 15. MANAGEMENT MANUAL. Banks shall have an operational risk management manual incorporating all risk management policies, duties and responsibilities of each involved area, and the means and frequency in which the Board of Directors and top management must be informed about operational risk management exposure.

Since all bank employees are involved in operational risk management, the operational risk management manual must be made available to them through the dissemination method the bank deems appropriate.

Banks must submit the operational risk management manual to the Superintendency no later than 31 January of each year. They must also submit updates or changes to this manual in a timely manner, using the same electronic means.

CHAPTER IV
RESPONSIBILITIES

ARTICLE 16. BOARD OF DIRECTORS. The Board of Directors of the bank is responsible for guaranteeing an appropriate environment for operational risk management, as well as fostering an internal environment that facilitates its development. Among their specific responsibilities are:

1. Approve the operational risk management policies and the relevant methodology;

2. Approve business continuity plans that permit the entity to react effectively to adverse situations;

3. Approve the necessary resources for the development of an appropriate operational risk management process, in order to have the necessary infrastructure, methodology and staff;

4. Ensure that the risk committee complies with the operational risk duties assigned to it;

5. Know the exposures and the main operational risk principles taken by the bank;

6. Know the required regulatory capital for operational risk and its effect within the bank;

7. Ensure that the bank has an effective operational risk management and that it is within the established tolerance limits;

8. Require periodic reports from the risk committee on operational risk exposure levels, their implications and mitigation plans;

9. Ensure that the matters discussed and the decisions made on operational risk management are fully documented in the board of directors meeting minutes.

ARTICLE 17. RISK COMMITTEE. The risk committee established pursuant to the Rule on Comprehensive Risk Management issued by the Superintendency of Banks is responsible for ensuring the bank's risk management is sound. It will perform the following duties, as a minimum:

1. Evaluate and propose the operational risk management manual, policies, procedures and methodologies for the approval of the board of directors;

2. Ensure that an appropriate operational risk management process is maintained and keep the board of directors informed on its effectiveness;

3. Ensure that operational risks are effectively and consistently identified, measured, mitigated, monitored and controlled. The result of this task will be documented in the risk committee meeting minutes when operational risk matters are discussed;

4. Follow up on risk exposures and compare these exposures with tolerance limits approved by the board of directors;

5. Define the scenarios and temporary horizon for the analysis of operational risk behavior. For these purposes, the risk management unit will be required to provide the relevant periodic reports;

6. Inform the board of directors about the exposures versus the limits established and the main operational risk taken, in addition to the historical behavior of these risks. This will require the risk management unit to present the corresponding periodic reports;

7. Inform the board of directors of any changes in the entity's risk profile and the results of operational risk, legal and regulatory indicators;

8. Review the regulatory capital requirement for operational risk and its effect on the bank;

9. Evaluate and approve action plans to implement the corrective actions required if there are deviations from the established limits;

10. Propose the business continuity plan for efficiently handling interruptions or situations that may create instability in the bank's operations or services for the approval of the board of directors;

11. Support the work of the risk management unit in implementing operational risk management;

12. Fully document the matters discussed and the decisions made on operational risk management in the risk committee meeting minutes;

13. The duties and requirements the board of directors may establish.

ARTICLE 18. TOP MANAGEMENT. Top management is responsible for implementing the risk management program approved by the board of directors. The responsibilities include the following:

1. Ensure consistency between operations and risk tolerance levels;

2. Establish review programs for the risk management unit and business units related to objectives, procedures and control compliance when conducting operations, as well as exposure limits and operational risk tolerance levels;

3. Ensure that the risk management unit has a sufficient budget to perform its duties;

4. Ensure that appropriate information storage, processing and management systems are in place;

5. Ensure that training and updating programs for the bank's risk management unit staff and all the personnel involved in operational risk-implied operations are established;

6. Establish procedures that ensure an adequate flow, quality and timeliness of information between the bank's business units and the risk management unit and to all other person involved in operations involving operational risk;

7. Create and foster an organizational culture of operational risk management and establish appropriate internal control practices, including standards of behavior, integrity and ethics for all employees;

ARTICLE 19. RISK MANAGEMENT UNIT. Pursuant to the provisions set forth in the Rule on Comprehensive Risk Management, the risk management unit's duties include managing

operational risk. In addition to the responsibilities provided in the aforementioned Rule, the risk management unit shall:

1. Submit the suitable structure for operational risk management to the board of directors through the risk committee, appointing responsible parties or coordinators of the different functional units for operational risk management activities;

2. Design and implement the methods and tools for measuring operational risk, consistent with the degree of sophistication and the volume of its operations;

3. Coordinate the identification, measurement, monitoring, control, mitigation and reporting of relevant operational risks to which the bank is exposed with operational and administrative areas;

4. Ensure that responsible units furnish the information necessary to be used with the methods and tools to measure operational risks;

5. Report any and all deficiencies detected in the quality, timeliness and integrity of the information utilized by the risk management unit to the areas responsible for preparation and control;

6. Continually assess the models and tools for operational risk measurement, submitting the results to the risk committee;

7. Follow up on operational risk exposures and compare them to the limits approved by the board of directors;

8. Provide the information below to the risk committee or the responsible party on a quarterly basis:

    a. Exposures and deviations by operational risk type (Appendix 1) and business lines (Appendix 2) occurred compared to established operational risk limits;

    b. The impact on the regulatory capital adequacy for operational risk, considering the sensitivity analysis in different scenarios (stress testing), including external events;

    c. Suggestions on the remedial actions that could be implemented as a result of a deviation regarding the tolerance limits established;

    d. Historical evolution of operational risk taken by the bank with regard to the established tolerance limits;

    e. Behavior of the operational risk profile, indicators and maps;

    f. Opinion on the operational risk identified in new bank products or services, prior to their launch;

    g. Results of the monitoring tasks;

    h. Progress of tasks compared to the annual work plan.

9. Investigate and document the causes behind the deviations from established limits, and report [the results] in a timely manner to the risk committee, manager or administrator and the person responsible for internal auditing duties;

10. Request the remedial actions for reducing exposures or losses caused by operational risks from the process owners, in addition to the action plans to strengthen internal control and organizational culture towards an appropriate operational risk management;

11. Send the result of the operational risk capital requirement as stated in this Rule, ensuring the quality of the data used;

12. Coordinate and evaluate the test of the business continuity plan with administrative and business areas and submit the report on the test results to the board of directors through the risk committee;

13. The duties and requirements established by the risk committee.

ARTICLE 20. INTERNAL AUDIT UNIT. The internal audit unit will evaluate compliance with the procedures used for operational risk management in accordance with the present Rule. In addition, it will evaluate the effectiveness of the controls according to the list of identified operational risks and, at the request of the risk management unit, those controls for which events and/or incidents require an evaluation.

The internal audit unit will also submit an annual report to the Superintendency of Banks detailing, by date and administrative or business unit, the findings (condition, cause, effect and recommendations) related to any operational risk that the audit unit has classified as medium or high risk or that has resulted in losses to the bank. The report will be submitted no later than January 31st of each year, using the electronic means and format the Superintendency may establish.

CHAPTER V
OTHER MANAGEMENT PROVISIONS

ARTICLE 21. BUSINESS CONTINUITY PLAN AND INFORMATION SECURITY PLAN. As part of an appropriate operational risk management, banks must implement a business continuity plan aimed principally at providing effective responses ensuring service and banking business continuity in situations that might cause an interruption or instability in their operations.

This business continuity plan must be tested once a year, as a minimum. The plan must be included in the operational risk manual.

Banks must also have an information security management system, oriented towards ensuring the integrity, confidentiality and availability of information.

ARTICLE 22. SELF-ASSESSMENTS. At least once (1) a year, banks must carry out a self-assessment to detect strengths and weaknesses in their control of banking operations and services, using the list of identified operational risks to which the bank is potentially exposed. To this end, the bank must document the self-assessment conducted.

ARTICLE 23. DATABASES. Operational risk management is a permanent and continuous process. Consequently, it is necessary for banks to design and implement centralized and high-quality databases to record, order, classify, and have available, information on the events and incidents, in addition to guaranteeing the staff involved in these processes is trained.

Databases must meet the following criteria:

1. Operational risk (events or incidents) originated anywhere in the bank must be recorded, and policies and procedures must be developed for their capture and communication.

2. As a minimum, the following information about each event and/or incident must be recorded:

    a. Category: event or incident;
    b. Type of occurrence;
    c. Identification code (assigned by the bank);
    d. Business line, according to Appendix 2 of this Rule;
    e. Another business line, according to Appendix 2 of this Rule;
    f. Origin;
    g. Affected product;
    h. Process or area to which it belongs;
    i. Type of risk (according to level one of Appendix 1 of this Rule);
    j. Risk cause (according to level two of Appendix 1 of this Rule);
    k. Description of the event (according to the examples provided in Appendix 1 of this Rule);
    l. Occurrence date or start date;
    m. Discovery date;
    n. Accounting registry date;

o. Amount exposed or amount involved;
p. Insurance recovery;
q. Other recoveries;
r. Total amount recovered
s. Related accounting item(s)
t. Status
u. Prior estimated periodicity;
v. Frequency from;
w. Frequency to;
x. Criticality of frequency;
y. Severity from;
z. Severity to;
aa. Severity level;
bb. Frequency value;
cc. Severity value

All events and incidents should have an exposure or involved amount recorded. For events in which quantification is difficult for the bank, the entity must estimate the potential loss according to the situation that has occurred.

Even risk events in which there are no losses constitute potential incidents that need to be assessed, measured, controlled and monitored from the perspective of adequate risk management.

These databases may be used as reference points in the self-assessments mentioned in Article 22 of this Rule.

ARTICLE 24. RISK RATING AGENCIES. Banks shall ask their risk rating agencies to include the operational risk management program applied by the banks in their operations in the agency's methodologies.

ARTICLE 25. BACKUP FOR POTENTIAL LOSSES. The Superintendency may establish capital requirements to cover operational risk, based on international standards and according to the situation in the banking center or of a particular bank.

CHAPTER VI
CAPITAL AND INFORMATION REQUIREMENTS

ARTICLE 26. DETERMINING OPERATIONAL RISK-WEIGHTED ASSETS. Operational risk-weighted assets are determined by multiplying the Business Index (IN, for its acronym in Spanish) amount, as defined in the Technical Appendix of this Rule, by 0.75.

ARTICLE 27. OPERATIONAL RISK CAPITAL REQUIREMENTS. Minimum operational risk capital requirements are determined by multiplying the operational risk-weighted assets established above by the capital coefficient for the due date. The calculation should be made on a quarterly basis following the operational rules established by the Superintendency.

ARTICLE 28. REPORTING REQUIREMENTS. Banks shall submit an annual report containing the main issues and results of the operational risk management program, electronically and in the format the Superintendency provides, by January 31 of each year.

ARTICLE 29. ADDITIONAL REQUIREMENTS. Banks will make available to the Superintendency any information, database, policies, processes, procedures, management systems, strategies, plans, and others mentioned in this Rule, as well as reviews by auditors and the parent company if the parent company is abroad.

The Superintendency may also ask any bank for any additional information it deems necessary for appropriate operational risk supervision.

ARTICLE 30. TRANSPARENCY. Banks must disclose the basic aspects of the operational risk management conducted by the entity, including objectives and achievements, in their annual report, website or any other means available to the public.

CHAPTER VII
SANCTIONS

ARTICLE 31. SANCTIONS. The Superintendency will apply the sanctions established in Title IV of the Banking Law for noncompliance with the provisions contained in this Rule.

CHAPTER VIII
FINAL PROVISIONS

ARTICLE 32. REPEAL. With the enactment of this Rule, Rule 7-2011 dated 20 December 2011 and all its amendments will be repealed.

ARTICLE 6. ENACTMENT. This Rule will become effective on 31 December 2019. The pertinent reports must be submitted by 30 January 2020.

Given in the city of Panama on the eleventh (11th) day of September, two thousand eighteen (2018).

FOR COMMUNICATION PUBLICATION AND ENFORCEMENT.

THE CHAIRMAN,	**THE SECRETARY,**
Luuis Alberto La Rocca	Joseph Fidanque III

TECHNICAL APPENDIX[2]

The Business Index (IN) is defined as follows [(all acronyms are Spanish acronyms)]:

IN = CIAD + CS + CF

CIAD is the interest, leasing and dividend component
CS is the service component
CF is the financial component

At the same time, each of these components is defined as follows:

CIAD = Min (ABS(IINT-GINT); 0.0225 x SACD) + DIV

ABS(x-y) is the absolute value of x – y within the parentheses
Min (x; y) is the value of the lesser of the two quantities x and y
Max (x; y) is the value of the greater of the two quantities x and y.
IINT is the amount of interest income
GINT is the amount of interest payment
SACD is the balance of credits and debt recorded in the assets
DIV is the amount of dividends collected

CS = MAX (OIO; OGO) + Max (IHC; GHC)

OIO is other operating interest
OGO is other operating expenses
IHC is the income from fees and commissions
GHC is the expenses from fees and commissions

$CF = ABS (G_{CN} – P_{CN}) + ABS (G_{LB} – P_{LB})$

G_{CN} is the earnings from the trading portfolio
P_{CN} is the losses from the trading portfolio
G_{LB} is the earnings from the banking book
P_{LB} is the losses from the banking book

The description of the composition of the variables is as follows:

SACD is the amount of the balance of credits and debt recorded in the assets
SACD = SD + SCR + SIV + SR
SD is the balance of deposits in banks and other financial institutions
SCR is the balance of loans granted
SIV is the balance of investment in debt securities
SR is the balance of repos

The calculation of the Business Index for a given quarter will be made as follows:

- For the variables that are part of Profits, the amounts for each of the three months of the quarter will be added together and multiplied by four to annualize the value.

- For the variables that are Balance account items and are part of the SACD variable, the arithmetic average for the three months of the quarter will be calculated.

The following loss and profit account items do not contribute to any IN items:

- Insurance and reinsurance business income and expenses;
- Paid premiums and reimbursements/payments received from purchased insurance and reinsurance policies;
- Administrative expenses, including staffing, outsourcing fees paid for providing nonfinancial services (e.g. logistics, IT or human resources) and other administrative expense (e.g. IT expenses, utilities, telephone, travel, office supplies, mail service);

[2] Amended by Article 1 of Rule 3-2019 dated 30 April 2019.

- Recovery of administrative expenses, including recovery of customer accounts payable (e.g. taxes charged to customers);
- Expenses of business locales and fixed assets (except those resulting from operating risk loss events);
- Amortization of tangible and intangible assets (except amortization related to operational leasing assets, which must be included in financial leasing and operational expenses);
- Provisions or reversal of provisions (e.g. pension disbursements, commitments and collateral provided) except for provisions related to operating risk loss events;
- Expenses for social capital refundable on demand;
- Deterioration of value or reversal of deterioration of value (e.g. financial assets, nonfinancial assets, investments in affiliated companies, joint ventures or related companies);
- Variation of the trading fund recognized in Profit;
- Corporate taxes (taxes on profits, including current and deferred taxes)

APPENDIX 1

OPERATIONAL LOSS BY TYPE OF RISK

Type of risk (Level 1)	Cause of risk (Level 2)	Examples
Internal fraud	Unauthorized activities	(Intentionally) undisclosed operations, unauthorized operations (with monetary losses), (intentional) incorrect valuation of positions.
	Theft and fraud	Theft, embezzlement, forgery, bribery, account misappropriation, smuggling, (intentional) tax evasion.
External fraud	Robbery, theft and fraud	Robbery, forgery.
	Systems security	Damages due to cyberattacks, information theft.
Labor relationships and safety in the workplace	Labor relationships	Issues concerning wages, benefits, termination of contracts.
	Hygiene and safety in the workplace	Cases related to hygiene and safety standards in the workplace; employee indemnification.
	Diversity and discrimination	All kinds of discrimination.
Clients, products and business practices	Appropriateness, disclosure of information and reliability	Breach of trust / breach of guidelines, appropriateness concerns / disclosure of information (know your customer, etc.), breach of privacy of information about retail clients, breach of privacy, aggressive sales, misuse of confidential information.
	Unfair marketing practices	Restrictive practices of competition, improper commercial/marketing practices, manipulation of the market, misuse of confidential information (for the benefit of the company), money laundering.
	Defective products	Defects in the product (not authorized, etc.)
	Selection, sponsorship and risks	Absence of customer investigation pursuant to guidelines, exceeding customer risk limits.
	Consultancy activities	Lawsuits on the results of consultancy activities.
Damages to physical assets	Natural disasters and other events	Losses due to natural disasters, human losses due to external events (terrorism, vandalism).
Business interruption and system failure	Systems	Losses due to hardware, software or telecommunications systems failure; power failures
Deficiency in execution, delivery and process management	Receiving, execution and maintenance of operations	Maintenance or discharge, failure to comply with deadlines or responsibilities, systems. Errors in securities and cash settlements.
	Follow-up and reporting	Failure to comply with reporting, inaccuracy of external reports (generating losses).
	Customer acceptance and documentation	Lack of customer authorizations / customer rejections; missing/incomplete legal documents.
	Customer account management	Unauthorized access to accounts, incorrect customer records (generating losses), losses or damages to customer assets due to negligence.
	Commercial counterparties	Failure of counterparties other than customers, other lawsuits with counterparties other than customers.
	Distributors and suppliers	Outsourcing, lawsuits with suppliers.
Legal		Losses arising from penalties imposed for failure to comply with standards, laws and regulations. Also as consequences from lawsuits against the bank resulting in the return of money to third parties.

Type of risk (Level 1)	Cause of risk (Level 2)	Examples
Deficiencies in management information	Incorrect assumptions	Exaggerated optimism about economic growth. Any other incorrect assumption that has affected bank decisions.
	Biased indicators	Liquidity index. Any other indicator the bank uses.
	Deficient information	Lack of awareness of profitability per client. Any incomplete or incorrect information.
	Unconfirmed analysis	Unconfirmed analysis on competitors. Any lack of comparison or verification.
Deficiencies in models	Incorrect assumptions	Using models obtained in other contexts.
	Deficiencies of data	Failure to update the value of collaterals. Any incomplete or incorrect information.
	Biased estimates	Estimate of probabilities without the appropriate sample and without previously having a verified qualification system.
	Lack of confirmation	Coverage models without an efficacy evaluation.

APPENDIX 2

GENERIC BUSINESS LINES FOR FINANCIAL SYSTEM CORPORATIONS

Type of risk (Level 1)	Cause of risk (Level 2)	Examples
Corporate finance	Corporate finance	Conducting structured funding operations and involvement in securitization processes; underwriting; financial advisory to corporations, big and medium enterprises, central government and public sector institutions; and other similar activities.
	Public administration finance	
	Investment banking	
	Advisory services	
Bargaining and sales	Sales	Treasury operations; purchase and sale of securities; currencies and commodities by the bank; among other similar activities.
	Market creation	
	Own positions	
	Treasury	
Retail banking	Retail banking	Retail loans and deposits; banking, trust funds and testamentary services.
	Private banking	Private loans and deposits, banking, trust funds and testamentary services and investment advisory.
	Card services	Private brand and retail corporate and business cards.
Commercial banking	Commercial banking	Loans for wholesaling customers, including: real estate, export funding, commercial funding, loans, collateral, bills of exchange, factoring and leasing, among others.
Payments and settlement	External customers	Activities associated with payments and collections, clearing and interbank fund transfers and settlements, among other similar activities.
Other services	Custody	Custodial services, trust funds
	Agency for corporations	Agents for issuers and payments
	Trust funds for corporations	
	Other services	
Asset management	Discretional asset management	Grouped, separated, retailing, institutional, closed, open, shareholdings
	Non-discretional asset management	Grouped, separated, retailing, institutional, fixed capital, variable capital
Retail intermediation	Retail intermediation	Complete execution and service