Republic of Panama
Superintendency of Banks

RULE No. 007-2011[1]
(dated 20 December 2011)

"Whereby the rules on Operational Risk are established"

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

CONSIDERING:

That due to the issuance of Decree Law 2 dated 22 February 2008, the Executive Branch published Decree Law 9 of 1998 and all its amendments as a single integrated text approved by means of Executive Decree 52 dated 30 April 2008 and hereinafter referred to as the Banking Law;

That, according to the provisions set for in paragraph 1 of article 5 of the Banking Law it is the objective of the Superintendency of Banks to safeguard the soundness and efficiency of the banking system;

That pursuant to Article 6 of the Banking Law, the duty of the Superintendency of Banks is to ensure that banks maintain liquidity and solvency rates adequate for the discharge of their obligations;

That according to the technical powers set forth in Article 11, Paragraph I, Subparagraph 5 of the Banking Law, it is the duty of the Board of Directors to establish the administrative interpretation and scope of the legal provisions and regulations on banking matters;

That according to the technical powers set forth in Article 11, Paragraph I, Subparagraph 3 of the Banking Law, it is the duty of the Board of Directors to approve general criteria for the classification of assets at risk and rules for the provision of reserves against risks;

That pursuant to the provisions set forth in Article 72 of the Banking Law on the assessment of other risks, it was established that in determining the capital adequacy ratio, the Superintendency may take into account the presence of other risks, including market risks, operating risks, and country risks;

That pursuant to the provisions set forth in Article 16, Paragraph I, Subparagraph 22 the Superintendent of Banks has a duty to evaluate the financial indicators of banks and banking groups to permit an adequate follow-up of the principal banking risks, including capital adequacy, credit liquidity, operating and market risks and others that the Superintendency may consider appropriate;

That the 7th Principle of an effective banking supervision of the Basel Committee, establishes that banks must have a comprehensive risk management process, including vigilance by the board of directors and top management to identify, assess, monitor and control or mitigate all substantial risks and assess their overall capital sufficiency with respect to their risk profile;

[1] Amended by Rule 11-2014 dated 14 October 2014.

That according to their characteristics, operations, and products offered, banks take operational risks and therefore they must evaluate this risk within their risk management process;

That during the Board of Directors' working sessions it became obvious that it was necessary and advisable to create a rule establishing a general framework for operational risk management.

RESOLVES:

OPERATIONAL RISK MANAGEMENT STANDARD

CHAPTER I
GENERAL PROVISIONS

ARTICLE 1.- PURPOSE 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 of this Rule are applicable to:

1. State-owned banks.
2. General license banks.
3. International license banks for which the Superintendency is home supervisor.

International license banks for which the Superintendency is host supervisor must establish an appropriate operational risk management system within their internal structure that will be subject to the Superintendency's inspection. Notwithstanding the above and when deemed advisable, the Superintendent may require the local management of the bank to follow the operational risk management requirements set forth in this Rule.

ARTICLE 3.- TERMS AND DEFINITIONS. The following definitions are noted for the application of the provisions contained in this Rule:

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 top executive officer (general manager, executive vice president, chief executive officer, etc.), as well as the second most senior executive (deputy general manager, etc.) and other managers and employees performing key duties and reporting directly to the two senior executives.

3. **Comprehensive Risk Management.** The process whereby the bank identifies, measures, monitors, controls, and mitigates the different types of risks to which the bank is exposed to according to the size and sophistication of its operations, products and services, and informs the operating groups within the bank.

4. **Operational risk.** The possibility of incurring losses due to deficiencies, failures or inadequacies of human resources, processes, technology or infrastructure, or due to external events. This definition includes the legal risks related to such factors.

5. **Legal Risk:** The possibility of incurring financial losses from a breach of rules, regulations or procedures with potential legal consequences, as well as due to contractual provisions. Legal risk also arises from malicious, negligent or unintentional acts affecting the execution, effectiveness or performance of contracts or transactions.

6. **Operational Risk Event.** An internal or external event or series of potential events whose occurrence could result in financial losses for the bank.

7. **Operational Risk Incident.** An internal or external event or series of events that has occurred and that may result in financial losses to the bank.

8. **Operational Risk Factor.** The primary cause or origin of an operational risk event. Factors may be **internal** (human resources, processes, technology or infrastructure, over which the organization has direct control) or **external** (events over whose causes or origin the organization has no control).

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

CHAPTER II
APPROPRIATE ENVIRONMENT FOR OPERATIONAL RISK MANAGEMENT

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

As set forth in the Rule on Comprehensive Risk Management, the organization 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 managing operational risk. Thus, they must establish a methodology that will allow for the identification, measurement, mitigation, monitoring and control and reporting of said risk.

Taking into consideration that all bank divisions produce potential operational risk events, the strategy must have the support of the board of directors and involve all staff.

The strategy used must be periodically updated based on risk tolerance, market changes and the economic environment that could affect the bank's operations. It is also important that the strategy define or identify adequate resources in terms of trained staff, processes, information systems and the necessary environment for operational risk management.

ARTICLE 6.- POLICIES. Banks must develop operational risk policies, 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. The manner and schedule for informing the board of directors, top management and others of the operational risk exposure of the bank and each of its business units.

3. The acceptable level of risk for the bank, according to the type and severity of the risk.
4. The process that must be followed, among other requirements, for the approval of new operations, products and services.
5. Operational risk indicators defined by the bank.

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, including: lack of trained staff, negligence, human error, sabotage, fraud, robbery, misappropriation of sensitive information, nepotism, inappropriate interpersonal relationship, unfavorable working environments, and lack of clear specifications in staff contracts, among others.

2. **Internal Processes.** For the purpose of guaranteeing the optimization of resources and 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 guarantees the acquisition, processing, storing, and reporting of information in a timely and reliable manner; that prevents business interruption; and that 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 Events.** 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 consideration the risk of legal contingencies, the failure of public services, natural disasters, attacks and criminal activity, and failures in services provided by third parties.

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 bank must identify operational risk events and incidents, grouping them as follows:

1. **Internal fraud.** Losses incurred by fraud, misappropriation of property or noncompliance with regulations, laws or internal policies by bank employees.

2. **External fraud.** Losses incurred by fraud, misappropriation of property or noncompliance with legislation by third parties.

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

4. **Practices related to clients, products and business.** Losses caused by noncompliance with an obligation to clients or derived from the nature or design of a product or service. Also included 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.** Losses from damages to material assets as a result of natural disasters or other events.

6. **Business interruption due to information technology failure.** Losses from business interruption and systems failure.

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

The identification of operational risk events or incidents must be grouped by type of risk, pursuant to the provisions set forth in Appendix 1. Also, it is advisable to identify these loss events by group according to the bank's business lines, as explained in Appendix 2.

ARTICLE 10.- MEASUREMENT. As part of operational risk management, the bank must evaluate operational risk events and incidents. This involves measuring possible losses in terms of probability of occurrence (frequency) and impact (severity).

The assessment or measurement of operational risk events and incidents is important for the bank because the assessment can be used to establish coverage mechanisms such as capital requirements. Additionally, it is important because this assessment or measurement must be used to establish preventive measures in order to minimize losses.

ARTICLE 11.- MITIGATION. As part of operational risk management, once the operational risk events and their frequency, as well as the institutional failures or vulnerabilities related to them are identified, top management must decide if the risk should be accepted, shared, avoided or transferred, reducing its consequences and effects.

Also, top management shall have a clear idea of the different types of exposures to operational risk and their priority, in order to make decisions and take actions. The possibilities include reviewing strategies and policies; updating or amending processes and procedures already established; implementing or modifying risk limits; creating, increasing or modifying controls; implementing contingency plans; reviewing the terms of current insurance policies; contracting third-party services; among others.

Top management must establish an action plan to implement measures to mitigate the risk events already identified. This plan must identify the actions to implement, the estimated time of execution and the persons responsible for their execution.

ARTICLE 12.- MONITOR AND CONTROL. As part of operational risk management, the bank must carry out monitoring to ensure that all actions implemented to mitigate a risk event are met within the established period and that the measures implemented have in fact contributed to the reduction of the risk of that event as well as a reduction in the overall risk for the institution.

ARTICLE 13.- REPORTING. As part of operational risk management, the bank must ensure that the Board of Directors and top management receive timely information on all risk management activity that is performed and the operational risk level to which the bank is exposed.

This stage also involves ensuring that operations divisions receive information on the events and their frequency periodically, in order to take 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 and comply with the following requirements:

1. Be fully documented.
2. Be implemented in all bank divisions.
3. Allow for the continuous improvement of operational risk management.
4. Be integrated with all of the risk management processes of the institution.
5. Establish procedures that ensure its compliance.
6. Be approved by the risk committee.

ARTICLE 15.- MANAGEMENT MANUAL. Banks shall have an operational risk management manual incorporating all risk management policies, duties and responsibilities of each involved group, and the manner 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, it is recommended that the operational risk management manual be available to them by a method the bank deems appropriate.

Banks must submit the operational risk management manual mentioned in this article to the Superintendency no later than 1 January 2013. They must also submit updates or changes to this manual in a timely manner.

CHAPTER IV
RESPONSIBILITIES

ARTICLE 16.- THE 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 policy and the relevant methodology.
2. Approve the necessary resources for the development of an appropriate operational risk management process, in order to have the necessary infrastructure, methodology and staff.
3. Ensure that the risk committee complies with the operational risk duties assigned to it.
4. Require and assess periodic reports from top management on operational risk exposure levels, their implication and relevant activities for their mitigation and/or suitable management.
5. Understand the main operational risks assumed by the bank and ensure an effective management and adequate criteria for establishing risk tolerance levels for their consequences and effects.
6. Ensure that the bank has an effective operational risk management system and that it is within established tolerance levels.

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

1. Review and present the operational risk management methodology for the approval of the Board of Directors.
2. Review, evaluate and present operational risk management policies for the approval of the Board of Directors.
3. Ensure that an appropriate operational risk management process is maintained and keep the Board of Directors informed on its effectiveness.
4. Ensure that all operational risks are effectively and consistently identified, measured, mitigated, monitored and controlled.
5. Propose mechanisms for the implementation of the required corrective actions should be there any deviations in regards to operational risk tolerance levels.
6. Support the work of the risk management unit, in implementing operational risk management.

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. 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.
2. Manage the operational risk management process and ensure its integrity in accordance with the guidelines established by the Board of Directors.
3. Provide the necessary resources for operational risk management implementation.
4. Ensure that all operational risk management strategies and objectives are met.

ARTICLE 19.- THE RISK MANAGEMENT UNIT. Pursuant to the provisions set forth in the Rule on Comprehensive Risk Management, the risk management unit duties includes, managing operational risk. Besides the responsibilities established in the Rule above, the unit shall:

1. Design and submit the policies for operational risk management through the risk committee, for the approval of the Board of Directors.
2. Design and submit the methodology for operational risk management for the approval of the risk committee.
3. Present a suitable structure for operational risk management to the Board of Directors through the risk committee, identifying the persons responsible for, or the coordinators of, the different functional units for operational risk management activities.
4. Implement the operational risk management methodology.
5. Support operation and business divisions in implementing the operational risk methodology.
6. Prepare an opinion on potential operational risk involved with new products or services before their launch.
7. Report failures on different operational risk factors to the Board of Directors through the risk committee, providing complete and detailed information in a timely manner.

ARTICLE 20.- THE INTERNAL AUDIT UNIT. The internal audit unit shall evaluate compliance with the procedures used for operational risk management prepared in accordance with the provisions of this Article, as well as the effectiveness of controls established within the operational risk management framework.

CHAPTER V
OTHER PROVISIONS ON MANAGEMENT

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

ARTICLE 23.- DATABASES. Operational risk management is a permanent and continuous process. Consequently, it is necessary for banks to design and implement databases in which to collect all events and incidents in order to comply with the following criteria:

1. All loss events originating anywhere in the bank must be recorded. The bank must develop policies, capture procedures and training for the staff involved in the process and

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

    a. Category: event or incident
    b. Identification code (assigned by the bank).
    c. Type of risk (according to level 1 of Appendix 1 of this Rule).
    d. Business line involved, according to Appendix 2.
    e. Cause of risk (according to level 2 of Appendix 1 of this Rule).
    f. Event description. (According to the examples described in Appendix 1).
    g. Process or area to which it belongs.
    h. Occurrence or start date.
    i. Discovery date.
    j. Accounting registry date.
    k. Gross amount(s) of loss(es).
    l. Amount(s) recovered through the coverage in force prior the event (if applicable).
    m. Total amount recovered (if applicable).
    n. Accounting line(s) involved (if applicable).

In case of incidents involving multiple losses, banks must register the minimum information required for each loss and establish a way to group the information under the event that originated them.

In the case of an event in a category in which the losses are only estimated, the bank should begin by registering partial information and complete the entry if the event becomes an incident. For example, the bank could register first the loss amount and later include the amounts recovered.

Banks shall create databases in which to register risks that have not become losses but that require evaluation, measuring, control and monitoring from an appropriate operational risk management approach. These databases may be used as reference points in the self-assessments mentioned in Article 22 of this Rule.

ARTICLE 24[2].- Rescinded.

ARTICLE 25.- RISK RATING AGENCIES. Banks shall ask their risk rating agencies to include in their methodologies the operational risk management program applied by the banks in their operations.

ARTICLE 26.- BACKUP FOR POSSIBLE 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.

ARTICLE 27.- TRANSPARENCY. Banks must disclose in their annual report, website or any other medium available to the public, the basic aspects of the operational risk management carried out by the institution, including objectives and achievements.

CHAPTER VI
FINAL AND TRANSITORY PROVISIONS

ARTICLE 28[3].- REPORTING REQUIREMENTS. Banks shall submit an annual report containing the main points and the results of their operational risk management program to the Superintendency no later than 31 January of each year.

In addition, banks must submit a report on the events and incidents contained within the "databases" referred to in Article 23 herein by electronic means and in the manner and frequency the Superintendency may establish.

Banks must ensure that the annual report referred to in the first paragraph of this Article, includes the parameters contained in the rules the Superintendency provides in further developing this reporting requirement.

ARTICLE 29.- ADDITIONAL REQUIREMENTS. Banks shall have at the disposal of this Superintendency any information, databases, 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 overseas.

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

ARTICLE 30.- SANCTIONS. In case of noncompliance with the provisions contained in this Rule, the Superintendency will apply the sanctions established in Title IV of the Banking Law.

ARTICLE 24: ENACTMENT. This Rule shall become effective on the first (1st) of July, two thousand twelve (2012).

Given in the city of Panama on the twentieth (20th) of December, two thousand eleven (2011).

[2] Without effect as provided for in Article 1 of Rule 11-2014 dated 14 October 2014.
[3] Amended by Article 2 of Rule 11-2014 dated 14 October 2014.

LET IT BE KNOWN, PUBLISHED AND ENFORCED.

THE CHAIRMAN, **THE SECRETARY,**

Arturo Gerbaud De La Guardia Felix B. Maduro

APPENDIX N° 1

TYPES OF RISK DUE TO OPERATIONAL LOSS

Type of Risk (Level 1)	Cause of Risk (Level 2)	Examples
Internal fraud	Unauthorized activities	Undisclosed operations (intentional), unauthorized operations (with pecuniary losses), positions evaluated mistakenly (intentional).
	Robbery and fraud	Theft, embezzlement, forgery, bribery, misappropriation of accounts, smuggling, tax evasion (intentional).
External fraud	Theft, Robbery and fraud	Robbery, forgery.
	Security of systems	Damages from computer attacks, theft of information.
Labor relations and safety in the workplace	Labor relations	Issues related to pay, social benefits, termination of contracts.
	Hygiene and safety in the workplace	Cases related to hygiene and safety standards; indemnification of employees.
	Diversity and discrimination	Any type of discrimination.
Clients, products and business practices	Adequacy, disclosure of information and trust	Betrayal of trust/breach of guidelines, fitness aspects/disclosure of information (know your customer, etc.), breach of privacy of retail client information, breach of privacy, aggressive sales, abuse of confidential information.
	Unfair market practices	Restrictive competition practices, unfair commercial/market practices, market manipulation, abuse of privileged information (in favor of the company), money laundering.
	Defective products	Product defects (unauthorized, etc.), models errors.
	Selection, sponsorship and risks	Failure to investigate clients according to the guidelines, exceeding risk limits for clients.
	Advisory activities	Lawsuits resulting from advisory activities.
Damages to physical assets	Disasters and other events	Losses due to natural disasters, casualties due to external causes (terrorism, vandalism)
Business interruption and systems failure	Systems	Losses due to hardware, software or telecommunications malfunction; electrical failure.

Execution, delivery and process management	Reception, execution and maintenance of operations	Errors when inputting, maintaining or downloading data, noncompliance with deadlines or responsibilities, wrongful execution of models/systems, accounting errors. Errors in processing securities compensation and cash liquidation.
	Follow-up and submission of reports	Noncompliance in reporting, inaccuracy of external reports (generating of losses).
	Acceptance of clients and documentation	Lack of authorizations/rejections of clients, nonexistent/incomplete legal documentation.
	Management of client account	Unauthorized access to accounts, inaccurate client registries (generating losses), lost or damage of clients' assets due to negligence.
	Commercial counterparts	Failure of counterparts who are not clients, other lawsuits with counterparts who are not clients.
	Distributors and suppliers	Subcontracts, lawsuits with suppliers.
Legal		Losses due to penalties imposed due to noncompliance with laws or regulations. Also, as a consequence of lawsuits against the bank, which require the bank to reimburse third parties.

APPENDIX N° 2

GENERIC LINES OF BUSINESS FOR COMPANIES IN THE FINANCIAL SYSTEM

Level 1	Level 2	Definition
Corporate finances	Corporate finances	Carrying out structured funding operations and participation in securities processes; underwriting; financial advisory to corporations, large and medium-sized companies, as well as central government and public sector entities; other activities of a similar nature.
	Public Administration finances	
	Investment banking	
	Advisory services	
Trading and sales	Sales	Treasury operations; purchase and sale of securities, currencies and commodities for the bank; other activities of a similar nature.
	Market creation	
	Bank positions	
	Treasury	
Retail banking	Retail banking	Retail client loans and deposits; banking, trust fund and testamentary services.
	Private banking	Private loans and deposits; baking, trust fund and testamentary, and investment advisory services.
	Credit Card services	Business/commercial Cards issued as a private brand or by retailers.
Corporate banking	Corporate banking	Financing for nonretail clients, including: real estate, export funding, commercial financing, loans, pledges, letters of exchange, factoring, financial leasing, among others.

Payment and settlement	External clients	Activities related to payments and collections, interbank funds transfer, compensation and settlement, other activities of a similar nature.
Other services	Custodian	Custodial and trust fund services
	Agent for companies	Agents for issuers and payments
	Corporate Trust funds	
	Other services	
Asset management	Discretionary management of funds	Group, segregated, retail, institutional, closed, open, stakeholder
	Nondiscretionary management of funds	Group, segregated, retail, institutional, fixed capital, variable capital
Retail brokerage	Retail brokerage	Full service and execution