Republic of Panama
Superintendency of Banks

RULE No. 003-2012
(dated 22 May 2012)

"Whereby the Guidelines for Managing Information Technology Risks are Provided"

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 reedited Decree Law 9 of 1998 and all of its amendments as a sole text, and that this text was approved by means of Executive Decree 52 dated 30 April 2008, hereinafter referred to as the Banking Law;

That pursuant to paragraph 1 of Article 5 of the Banking Law, the objective of the Superintendency of Banks is to safeguard the soundness and efficiency of the banking system;

That pursuant to paragraph 2 of Article 5 of the Banking Law, an objective of the Superintendency of Banks is to strengthen and foster favorable conditions for the development of the Republic of Panama as an international financial center;

That pursuant to the provisions of Article 11, Paragraph 5 of the Banking Law, it is the technical responsibility of the Board of Directors to interpret and establish the scope of the legal provisions on banking matters within the administrative sphere;

That pursuant to Article 11, Paragraph 10 of the Banking Law, it is the technical duty of the Board of Directors to issue the technical standards required for compliance with the Banking Law;

That pursuant to the provisions set forth in Article 16, Paragraph 22, it is the technical duty of the Superintendent to evaluate the financial indicators of banks and banking groups to permit an adequate monitoring of the principal banking risks such as capital adequacy, credit, liquidity, operating and market risks, and other risks that the Superintendency may consider appropriate;

That by Rule 008-2010 dated 1 December 2010 the Superintendency established the provisions for Comprehensive Risk Management, whereby banks are required to identify and manage all risks to which they are exposed, in accordance with the size and complexity of their operations, products and services;

That in Rule 005-2011 dated 20 September 2011 the Superintendency updated the provisions on Corporate Governance, setting forth clear guidelines for the organization of corporate governance within banks;

That the minimum parameters for operating risk management were provided by Rule 7-2011, which in Article 7 indicates that information technology is a risk factor or category, and that because of its nature it requires specialized management;

That the 7th principle of the Basel Committee's Core Principles for Effective Banking Supervision establishes that banks must have in place a comprehensive risk management process, including Board and senior management oversight, to identify, evaluate, monitor

and control or mitigate all material risks and to assess the bank's overall capital adequacy in relation to its risk profile;

That the rapid development of technology involves benefits and risks in banking operations; therefore it is necessary to set forth minimum guidelines for managing information technology-related risks according to international best practices;

That during the Board of Directors' working sessions it became obvious that it was necessary and advisable to establish minimum criteria for managing information technology-related risks.

RESOLVES:

CHAPTER I
GENERAL PROVISIONS

ARTICLE 1. SCOPE OF APPLICATION. The provisions of this Rule shall be applicable to state-owned, general license and international license banks to which the Superintendency is the home supervisor.

ARTICLE 2. DEFINITIONS. For the purposes of this Rule, the following terms shall be defined as:

1. **Information technology governance:** the set of processes, responsibilities, policies, procedures, relationships and controls supporting business goals, optimizing investment and managing information technology-related risks and opportunities.
2. **Information technology risk:** the possibility of economic losses as a consequence of an event related to technology infrastructure or the unauthorized access or misuse of technology, affecting the performance of business processes or bank risk management, by compromising confidentiality, integrity, availability, efficiency, reliability, compliance or the timely use of information.
3. **Information Technology or "IT":** the set of technology instruments that permits the purchase, production, storing, treatment, communication, registration, access and submittal of information.
4. **Security of information:** the preservation of the confidentiality, integrity and availability of information and of the other IT resources of the organization. It also, includes the compliance with laws, regulations, agreements, rules and contracts associated with the use and management of IT resources and the overall management of information.

CHAPTER II
INFORMATION TECHNOLOGY GOVERNANCE

ARTICLE 3. IT GOVERNANCE. Banks must have an organizational structure in accord with their size, the complexity of their operations and their risk profile, permitting the management of IT and its related risks.

IT governance must establish policies, strategic plans and procedures, as well as allocating the resources necessary to manage IT. These must be continuously reviewed and evaluated, focusing on the following items as a minimum:

1. **Strategic Alignment**: preparing an IT strategic plan defining IT initiatives aligned to the business's goals, plans and operations. Short-, medium- and long-term IT objectives, activities and projects must be identified.

2. **Value delivery**: managing IT to ensure that it provides the benefits projected in the strategic plan.

3. **Resource management:** managing IT resources, such as human resources and technology infrastructure optimally and appropriately, and ensuring the proper execution and control of a budget for managing those resources.

4. **Risk management**: identifying, understanding and managing risks to which the bank is exposed, as well as determining its risk tolerance. To achieve this, the bank must have an IT risk management methodology which includes the design of a risk matrix and guarantees systems security. This will include, as a minimum, control measures for logic security (system access controls), physical security and network security.

5. **Performance Appraisal**: providing continuous monitoring of the implementation of the IT strategy through a constant assessment of process performance and the attainment of IT objectives and goals, as well as the completion of projects, the use of resources and service delivery.

ARTICLE 4. CRITERIA FOR IT CONTROL. Banks must define IT objectives that are aligned with their business objectives. To this effect, banks shall apply specific IT controls conforming to the following criteria:

1. **Effectiveness:** the information and related processes should be relevant and appropriate to compliance with their objectives. Information must be submitted in an appropriate manner permitting its timely use.

2. **Efficiency:** the resources for the application of information processes must be optimized.

3. **Confidentiality:** information must be protected from unauthorized access and use.

4. **Integrity:** the information must be complete, accurate, reliable and truthful.

5. **Availability:** timely and organized access to information.

6. **Compliance with Standards:** the information must comply with internal policies, contractual stipulations and applicable laws and regulations.

ARTICLE 5. RESPONSIBILITIES OF THE BOARD OF DIRECTORS. The board of directors of the bank is responsible for:

1. Approving the IT strategic plan and the business continuity plan.

2. Overseeing the determination of and compliance with the organizational structures, policies and procedures necessary for managing IT and its related risks in accordance with the size, nature, and complexity of the operations carried out by the bank.

3. Ensuring that IT governance is appropriately managed as part of corporate governance.

4. Ensuring periodic audits for the continuous assessment, review and monitoring of IT functions and operations.

5. Approving IT investment priorities pursuant to business objectives.

ARTICLE 6. IT COMMITTEE. All banks must have an IT committee to oversee the bank's IT management.

The IT committee shall be composed of senior management, the business divisions and the division responsible for IT. The number of members comprising this committee will depend on the bank's size and complexity.

The IT committee shall prepare its internal work regulations and shall have the policies and procedures needed to comply with its functions. The regulations will be adapted to the provisions issued by the Superintendency, including this Rule, and shall establish the frequency of its meetings and the information related to IT governance that must be submitted to the board of directors, among other aspects.

Based on its organizational structure, banks may request a waiver of the provisions of this article from the Superintendent as long as the bank proves to the satisfaction of the Superintendency that there will be an entity responsible for covering the responsibilities of the IT committee.

ARTICLE 7. RESPONSIBILITIES OF THE IT COMMITTEE. The duties of the IT Committee are:

1. To propose an IT strategic plan aligned to the bank's business strategy for the approval of the board of directors.

2. To propose IT investment priorities pursuant to the bank's business objectives for the approval of the board of directors.

3. To monitor the IT projects being executed according to the IT strategic plan.

4. To supervise the level of IT service.

CHAPTER III
IT RISK MANAGEMENT

ARTICLE 8. IT RISK MANAGEMENT. Banks must identify, measure, monitor, control, mitigate and report IT risks to operational divisions exposed to them in accordance to the size and complexity of their operations, products and services.

ARTICLE 9. RISKS COMMITTEE. In addition to the other risks for which it is responsible, the risk committee established in the Rule on Comprehensive Risk Management will be responsible for information technology risk management. To this end, it will be in charge of the implementation, proper functioning and execution of approved policies and procedures and will have the following duties:

1. To propose IT risk management policies and procedures and the business continuity plan for the approval of the board of directors.

2. To propose the IT risk management manual and relevant updates for the approval of the board of directors.

3. To analyze proposals for updating policies and procedures, the IT strategic plan, the business continuity plan and its testing plan, and to propose necessary updates to the board of directors.

4. To define the strategy for implementing approved IT risk management policies and procedures and their compliance.

5. To review IT risk management policies and procedures, as a minimum on an annual basis, and to propose updates, when applicable.

ARTICLE 10. UNIT RESPONSIBLE FOR RISK MANAGEMENT. The risk management unit (or other existing equivalent unit) in the bank will have among its functions IT risk management. In addition to the responsibilities set forth in the Rule on Comprehensive Risk Management, it shall comply with the following:

1. To manage IT risk.

2. To analyze, review and implement necessary technology and operating controls for adequate management of risks related to IT innovations to be implemented in the bank, as well as new products and services proposed by the business divisions.

ARTICLE 11. INFORMATION SECURITY UNIT. The Information Security Unit was created pursuant to the provisions of the Rule on E-banking to oversee the security of information. It will have among its duties the following, as a minimum:

1. To establish, review and update policies, norms, and procedures according to international standards on information security.

2. To ensure the security of the technology environment, carrying out risk assessments of the bank's applications and technology equipment.

3. To protect systems against new threats and existing vulnerabilities.

4. To ensure that the bank is not adversely affected by new threats, ensuring the availability of the systems needed to provide the services.

5. To keep security personnel trained and updated.

6. To establish communication with information security staff of other banks for the purpose of working together to strengthen banking system's security.

7. To coordinate analysis and penetration and vulnerability tests within the bank's technology environment.

8. To establish guidelines and standards for the control of access to information systems and for the modification of privileges and user profiles.

9. To participate in maintaining and updating the contingency plans, business continuity plans and disaster recovery plans to maintain the proper level of security during recovery activities.

10. To monitor and attend to information security incidents.

11. To notify the Superintendency of any attacks suffered, using the established format.

ARTICLE 12. BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN. All banks must ensure that their business continuity plan, as established in the Rule on Operational Risk Management, includes the following aspects related to IT:

1. Resistance tests designed to mitigate the impact of a major interruption in the key functions and processes of the business.

2. Alternate procedures, including adequate backup of the information and systems.

3. The ability to recover critical IT services.

4. Communication processes and test focus.

ARTICLE 13. INTERNAL AUDIT. All banks must ensure that their internal audit units have the resources and tools necessary to carry out the audits and assessments of all IT elements according to the size and complexity of their operations, so as to determine their deficiencies and potential solutions.

ARTICLE 14. OUTSOURCING. All banks outsourcing their IT functions or processes must ensure that they conform to the provisions stipulated in the Rule on Outsourcing issued by the Superintendency of Banks.

Additionally, the bank must ensure that the following conditions are included in the outsourcing agreement:

1. The obligation of the contracted company to allow the Superintendency of Banks access to IT infrastructure, information systems and databases (to the extent allowed by the Banking Law) related to the service outsourced by the bank, when the Superintendency requires it.

2. The obligation of the contracted company to submit to the bank all of the information required by the Superintendency (to the extent allowed by the Banking Law) relative to the service outsourced by the bank.

CHAPTER IV
FINAL PROVISIONS

ARTICLE 15. SANCTIONS. Failure to comply with the provisions contained herein will be punished by the Superintendent according to the provisions of Title IV of the Banking Law.

ARTICLE 16. ENACTMENT. This Rule shall enter into effect on the first (1st) of January, two thousand thirteen (2013).

Given in the city of Panama, on the twenty-second (22nd) day of May, two thousand twelve (2012).

LET IT BE KNOWN, PUBLISHED AND ENFORCED.

THE CHAIRMAN, **THE SECRETARY,**

Arturo Gerbaud De La Guardia Félix B. Maduro