

FINANCIAL SUPERVISORY COMMISSION



Cook Islands

PRUDENTIAL STATEMENT

No. 10-2009

POLICY FOR MANAGEMENT OF OPERATIONAL RISK

ISSUED UNDER SECTION 14(3) OF THE BANKING ACT 2003

1. This Prudential Statement is issued by the Financial Supervisory Commission (FSC) pursuant to the provisions of Section 14 of the Banking Act 2003 and shall be applicable to all bank licensees incorporated in the Cook Islands.
2. The Prudential Statement outlines a set of principles that provide a framework for the effective management of operational risk by banks. In this Prudential Statement, operational risk is defined and recommendations are outlined on the basis of the standards contained in the paper issued by the Basel Committee on Banking Supervision in February 2003, entitled *Sound Practices for the Management and Supervision of Operational Risk*.
3. The requirements established in this Prudential Statement constitute general requirements which a bank shall take into account in the arrangement of operational risk management conforming to the needs and options of the organization. The scope of application of the Prudential Statement depends on the organizational structure and culture, business volume and risk level of a bank, as well as on the legal complexity of the financial services and products offered by, and the characteristic features of risk management and accounting system of, the bank.

4. The FSC recognizes that some banks operate in the Cook Islands as branches of Australian banks, and that they do not have a Board in the Cook Islands. Their operational risk policies at Board level will therefore reflect the requirements of the Australian Prudential Regulation Authority. In the methodology that will be applied by the FSC for assessing operational risk management, the existence of requirements by the home regulator will be taken into account.

5. This guideline should be read in conjunction with the Banking Act 2003. The adoption and implementation of sound risk management practices re-assures a bank's depositors and engenders confidence in a bank.

BACKGROUND

6. Deregulation and globalization of financial services, together with the growing sophistication of financial technology, are making the activities of banks and thus their risk profiles (i.e. the level of risk across a firm's activities and/or risk categories) more complex. Developing banking practices suggest that risks other than credit, interest rate and market risk can be substantial.

7. Operational risk is a term that has a variety of meanings within the banking industry, and therefore for internal purposes, banks may choose to adopt their own definitions of operational risk. Whatever the exact definition, a clear understanding by banks of what is meant by operational risk is critical to the effective management and control of this risk category. It is also important that the definition considers the full range of material operational risks facing the bank and captures the most significant causes of severe operational losses.

8. Operational risk event types having the potential to result in substantial losses include:

- Internal fraud. For example, intentional misreporting of positions, employee theft, and manipulation of an employee's own account.
- External fraud. For example, robbery, forgery, credit card skimming and damage from computer hacking.
- Employment practices and workplace safety. For example, employers liability claims, violation of employee health and safety rules, organized labour activities, discrimination claims and general liability to the public.
- Clients, products and business practices. For example, fiduciary breaches, misuse of confidential customer information, improper trading activities on the bank's account, money laundering and sale of unauthorized products.

- Damage to physical assets. For example, cyclones, terrorism, vandalism, earthquakes, fires and floods.
- Business disruption and system failures. For example, hardware and software failures, telecommunication problems and utility outages.
- Execution, delivery and process management. For example, data entry errors, collateral management failures, incomplete legal documentation, unapproved access given to client accounts, non-client counterparty mis-performance and vendor disputes.

9. The diverse set of risks listed above can be grouped under the heading of 'operational risk', which the Basel Committee has defined as '*the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events*'. The definition includes legal risk but excludes strategic and reputational risk.

OPERATIONAL RISK MANAGEMENT

Identification of operational risk

10. Operational risk is a distinct risk area. Each bank shall formulate a definition of operational risk for its internal use. The definition of operational risk shall be based upon the scope and complexity of the business and previous experiences in the risk management of the bank and shall clearly articulate the factors that may cause an operational risk in the bank.

11. The content of a definition of operational risk shall be commensurate with the business practices of a bank (IT solutions used and complexity thereof; outsourcing, personnel policy, complexity of risk management relating to services and products offered; external insurance, etc.).

Arrangement of operational risk management

12. Operational risk management shall constitute an integrated part of the corporate governance and the general risk management system of a bank. Operational risk management shall be accompanied by improved definition and positioning of the activities of a bank, and transition from defensive activities to activities that involve the analysis of risks and prevention of loss events.

13. In the arrangement of operational risk management a bank should take into account that operational risk losses are not always measurable and they may be incurred after a substantial amount of time and/or indirectly.

14. Operational risk management is a process that requires a uniform understanding of operational risk organization-wide and it is based upon high organizational culture along with the relevant risk culture and positive attitude toward internal control. In operational risk management, the creation of unfounded "feeling of security" must be avoided, as this may entail the establishment of inappropriate objectives and unintended results (first of all as regards business continuity management).

15. In the application of this Prudential Statement, a bank shall seek to find a solution that is optimal and economically reasonable for its size and profile, while being in line with the scope of its business and comprising all legal and business units of the organizational structure. In the implementation of the requirements established in the Guidelines in the different units of a bank, excessive bureaucracy shall be avoided and the aim shall be efficiency of operational risk management and adding value to the entity.

16. The understanding of a bank of the operational risks inherent in its business and the willingness to pay attention to operational risk management besides conventional risk management systems and means (analysis models and programs, stress tests, etc.) are of essence.

17. The activities of a bank which relate to operational risk management should be subject to independent review and assessment.

DUTIES OF THE BOARD AND SENIOR MANAGEMENT

18. The duties of the Board include establishing the organizational, business and risk management structure which is appropriate for operational risk management, as well as general principles of supervising the activities of the bank.

19. Where the volume and scope of the business of a bank render it unreasonable to ensure the segregation of business and control structures, ways of risk mitigation by means of other measures shall be sought (e.g. additional controls, reporting, the so-called four-eyes principle, etc.).

20. It is the duty of the Board to ensure the creation of an internal control environment that supports efficient operational risk management involving all the units and activities of the bank.

21. The Board shall establish the definition of operational risk and the general principles (policy) of risk management and revise the same on a regular basis, taking into account, inter alia, changes in the activities and operating environment of the bank.

22. The Board shall, in conjunction with senior management, allocate the resources that are necessary for continuous development and implementation of

operational risk management (budgetary resources, motivated employees with relevant qualifications).

23. The Board shall be aware and have a clear understanding of the major operational risks inherent in the organization (IT, personnel), areas of activity and operating environment of the bank. The Board shall be provided with regular reports and overviews concerning the operational risk position of the bank, the circumstances that have caused changes in that position and, operational loss events.

24. The Board shall ensure the capability of the bank's internal audit function (qualified and motivated employees) to assess the internal regulations and activities that relate to operational risk management. The scope of activities of the internal audit function shall be sufficient to obtain assurance about the adequacy and efficiency of operational risk management. In the absence of an internal audit function, the scope of the external auditor will need to be expanded to include these activities.

25. While the internal audit function should not be directly responsible for particular activities relating to operational risk management, an optimal and economically reasonable solution should be found in conjunction with the risk management units, which corresponds to the bank's scope of activity and nature of risks.

26. Senior management shall design the organizational structure so as to ensure that areas of responsibility, reporting relationships and procedures of structural units are clearly identified. The segregation of the lines of accountability and reporting of the bank's business and control structures shall be ensured.

27. It is the duty of senior management to introduce processes in the bank which are based on sound risk management practices (the segregation of functions, the so-called four-eye principle, etc.), see to it that there is adherence to these processes, , and ensure the operation of the internal control environment, using regular reports and engaging internal audit, if appropriate.

28. Senior management shall be responsible for the implementation of the operational risk management principles (policy) approved by the Board within the bank. The operational risk management policy shall be implemented throughout the bank and all the levels of staff should understand their responsibilities with respect to operational risk management and ensure the performance of the related obligations.

29. Senior management is responsible for the development of sub-policies and internal regulations for management of operational risks inherent in all products, activities, processes and systems. While the manager of each structural unit is responsible for the appropriateness and efficiency of the operational risk

management principles and internal regulations within his or her purview, the senior management shall clearly determine the authority, liability and procedure for reporting in order to maintain that accountability.

30. Senior management should ensure that the operational risk management policy and the internal regulations for implementation thereof are communicated to all employees in all structural units that are exposed to operational risk. Employees' clear understanding of the risk management-related rights and obligations arising from their positions shall be ensured.

31. Senior management should also make sure that day-to-day activities relating to operational risk management are performed by qualified staff with sufficient experience and technical capabilities necessary for the work.

32. Employees responsible for monitoring and implementation of risk management in the bank need to have authority independent of the structural units and activities they oversee.

33. Employees responsible for operational risk management should consistently exchange information with employees responsible for credit, market and other risks.

34. It is expected that the bank's remuneration policy (wages, bonuses, benefits, etc.), will be consistent with the risk profile of the bank and support sound risk management practices and the internal control environment.

OPERATIONAL RISK POLICY

35. Operational risk policy should underlie the management of all the activities of the bank that relate to operational risks. The content of that policy should be commensurate with the scope and volume of the bank's business and cover all operational risks inherent in the activities of the bank.

36. Operational risk policy should contain references to areas relevant to operational risk management. These areas include, among others, physical security of the bank, manageability of IT systems, data protection, business continuity, prevention of money-laundering, personnel policy, etc.

37. Depending on the scope and volume of the bank's business and the nature of the services and products offered by it, the operational risk policy should identify the activities the purpose or contents of which have a direct or indirect impact on the bank's activities in operational risk management. Such activities include, e.g., the development of new products and services, the selection of external service providers, development activities (incl. IT), etc.

IDENTIFICATION AND ASSESSMENT OF OPERATIONAL RISKS

38. The identification and classification of operational risks must be based on a bank-wide understanding of operational loss events. A clear identification of loss events enables a bank to distinguish operational risk from credit and market risks and to quantitatively assess the operational risk.

39. A bank should identify and assess the operational risks inherent in all of its products, activities, processes and systems. It is also expected that a bank will ensure that before new products, activities, processes and systems are introduced or undertaken, the operational risks inherent in them are subject to adequate assessment procedures.

40. Effective risk identification considers both internal factors (such as the complexity of the organizational structure, the nature of the bank's activities, qualification of personnel, organizational changes and employee turnover) and external factors (such as changes in the industry and technological advances) that could adversely affect the achievement of the bank's objectives.

41. In addition to identifying the operational risks, a bank should also assess its vulnerability to these risks. Effective risk assessment allows the bank to better understand its risk profile and most effectively target risk management resources.

42. Examples of processes/activities used for identifying operational risks include:

- a) **Risk mapping:** in this process, various sub-units or owners of business or auxiliary processes of an organization map the risks inherent in their units/businesses/processes by risk type.
- b) **Risk assessment:** in this process, various sub-units or owners of business or auxiliary processes of the bank analyze the probability of occurrence and financial impact of a risk event (using the help of risk management staff and/or external consultants, if appropriate).
- c) **Key risk indicators:** risk indicators are statistics and/or metrics (measurements), often financial, which can provide insight into the risk position of a bank. These indicators are usually reviewed on a periodic basis (such as monthly or quarterly) in order to be aware of changes that may be indicative of risk concerns. Such indicators may include the number of failed transactions, staff turnover rates and the frequency and/or severity of errors and omissions.
- d) **Monitoring of thresholds/limits relating to risk indicators:** exceeding these thresholds/limits alerts the management to the existence of spheres with potential inherent problems.

43. Data on a bank's historical loss experience could provide information for assessing the bank's exposure to operational risk. An effective way of collecting and making good use of this information is to establish a classification for systematically tracking and recording the frequency, severity and other relevant information on individual loss events.

44. The classification developed by the Basel Committee on Banking Supervision could be used as a reasonable basis for the classification system. The classification system may differ across banks, but it should, as a general rule, comprise the following types of loss events:

- a) internal fraud;
- b) external fraud;
- c) employment practices and workplace safety;
- d) customers, products and business practices;
- e) damage to physical assets;
- f) business disruption and system failures;
- g) execution, delivery and process management.

45. The inclusion of operational loss events in individual classes in pursuance of the general nature of the operational loss events allows a bank to assess the risk mitigation measures employed for reducing the probability of occurrence and impact of those events. The system of classification of loss events should enable a bank to determine the types of events that might potentially result in material damage and provide direct information on the need for use, and the effectiveness and efficiency, of risk management measures.

46. In addition to the classification of operational risks by types of loss events, a bank should also classify loss events by types of principal fields of business. The fields of business underlying such classification may differ across companies.

47. Information about loss events principally comprises usual, high-frequency, low-severity events and low-frequency high-severity events. It would be reasonable to establish a reporting system that allows tracking and recording both types of loss events, including external information about material loss events.

48. High-severity events in a bank are generally accompanied by an improvement of the control system of the relevant sphere or activity (or the spheres or activities corresponding to the same criteria in the whole of the bank), which should substantially reduce the probability of occurrence of similar loss events in the future. In order to achieve a control environment that contributes to the prevention of loss events, it is important to take notice of high-severity loss events that have occurred in banks similar to the bank in question, and of the conditions and circumstances of occurrence of these loss events. This contributes to assessment of the probability of occurrence of similar loss events and testing the

operation of the bank's control environment and to material reduction of the probability of occurrence and/or financial impact of the loss events.

OPERATIONAL RISK MONITORING

49. An effective monitoring process is essential for ensuring adequate operational risk management. Regular monitoring of activities offers the advantage of quickly detecting and correcting deficiencies in the policies, processes and procedures for managing operational risk, and preventing losses.

50. In addition to monitoring operational loss events, a bank should identify and monitor the indicators that provide early warning of an increased risk of future losses. Such risk indicators (key risk indicators) should be forward-looking and reflect potential sources of operational risk such as rapid growth, the introduction of new products, employee turnover, interruptions in transactions and activities, system downtime, etc. When thresholds are directly linked to these indicators, an effective monitoring process can help identify key material risks in a transparent manner and enable the bank to act upon the (growing) risks appropriately.

51. Risk indicators may derive from the particular lines of business or comprise all of the areas of activity or units of a bank. Examples of such indicators include:

- a) the number of customer complaints;
- b) the number of customer compensation events;
- c) the number of interrupted transfers and transactions;
- d) employee turnover;
- e) the number of observations / precepts by supervisory authorities;
- f) the number of failures, or manageability, of (IT) systems;
- g) the number of internal policies and procedures in need of amendment.

52. Monitoring is most efficient if the control system is an integral part of the activities of a bank and if relevant regular reporting is stipulated. In addition to the reports to be submitted to the manager of the area in question, the results of such monitoring should be reflected in the reports submitted to senior management and the Board, as well. The contents of reports drawn up by supervisory function may also serve as input for the monitoring.

53. Senior management and the Board should receive regular reports from both business units and the internal audit unit (and the reports should be distributed to all the appropriate levels of management). The reports should contain internal financial, operational, and compliance data and fully reflect any identified problem areas and should motivate timely corrective measures.

54. To ensure the usefulness and reliability of these risk and audit reports, management should regularly verify the timeliness, accuracy and relevance of

reporting systems and internal controls in general, using reports prepared by external sources (auditors, supervisors) to that end. Reports should be analyzed with a view to improving existing risk management performance as well as developing new risk management policies, procedures and practices. Control and mitigation of operational risk.

55. A bank must have policies, processes and procedures in place to control and mitigate material operational risks. The appropriateness of alternative risk limitation and control strategies should be reviewed and the bank should adjust its operational risk profile accordingly using appropriate strategies, in light of the overall risk tolerance and profile of the bank.

56. Control activities need to be in place which are designed to address the operational risks that a bank has identified. For the risks that can be controlled, a bank should decide to what extent to use control activities and other appropriate measures, and to what extent it is prepared to accept these risks; that is, it should identify any risk mitigating factors and then examine the residual risks. For those risks that cannot be controlled, a bank should decide whether to accept these risks, reduce the level of business activity involved, or withdraw from this activity completely.

57. Control activities and procedures should be implemented for ensuring compliance with the established set of internal policies concerning the risk management system. Principal elements of this could include, for example:

- a) top-level reviews of the bank's progress toward the stated objectives;
- b) a system of documented approvals and authorizations to ensure that activities are carried out at an appropriate level of management;
- c) policies, processes and procedures concerning the review, treatment and resolution of non-compliance issues.

58. Although a system of formal, written policies and procedures is critical, control activities need to be carried out through a strong internal control function. To ensure efficiency, control activities should be an integral part of the regular activities of a bank, which makes it possible to quickly respond to changing conditions and avoid unnecessary costs.

59. An effective internal control environment requires appropriate segregation of duties and ensures that personnel are not assigned responsibilities which may create a conflict of interest. Assigning such conflicting duties to employees or to sub-units of the bank may enable them to cause losses or errors or carry out inappropriate actions. Therefore, potential conflicts of interest should be identified, minimized and be subject to independent monitoring and review. The relevant data should be included in risk reports.

60. In addition to segregation of duties, a bank should ensure that such other internal measures are in place as appropriate to control operational risk, such as close monitoring of adherence to assigned risk limits or thresholds; control of access to, and use of, assets and documents (ensuring security); ensuring that staff have appropriate expertise and training; identifying business lines or products where returns materially differ from expectations; and regular verification and reconciliation of transactions and accounts.

61. Operational risk can be more pronounced where a bank engages in new activities or develops new products (particularly where these activities or products are not consistent with the bank's core business strategies) or has entered unfamiliar markets. Owing to business objectives and customary preference thereof, there is a risk that a bank cannot ensure that its risk management infrastructure keeps pace with the growth in the business activity. Therefore, it is crucial in such a situation to ensure that special attention is paid to the development and operation of internal control functions.

62. Some significant operational risks have low probabilities but a potentially very large financial impact. While a bank cannot control all risk events (e.g., natural disasters), risk mitigation tools or activities can be used to reduce the frequency and/or severity of such events. For example, insurance policies, particularly those with prompt and certain pay-out features, can be used to externalize the risk of "low frequency, high severity" losses which may occur as a result of events such as third-party claims arising from errors or omissions, employee or third-party fraud, and natural disasters, etc.

63. A bank should view risk mitigation tools (incl. insurance policies) as complementary to, rather than a replacement for, internal operational risk control. Consideration also needs to be given to the extent to which risk mitigation tools truly reduce risk, or transfer the risk to another business area, or even create a new risk.

64. Investments in banking technology and information technology security are important for operational risk mitigation. Attention should be paid to the circumstance that increased automation could transform high-frequency, low-severity losses into low-frequency, high-severity losses. The latter may be associated with an interruption or extended disruption of business caused by internal or external factors. A bank should establish business continuity plans that address this risk.

OUTSOURCING¹

65. A bank should establish a policy for managing risks associated with outsourcing activities and determine the terms and conditions of selection of external service providers and of entry into contracts with them.

66. The board of Directors

- (a) must approve the Bank's outsourcing policy and keep it under review; and
- (b) is responsible for ensuring that –
 - (i) outsourcing decisions are taken; and
 - (ii) outsourced activities are undertaken;
in accordance with the Bank's outsourcing policy.

67. In the selection of external service providers, a bank should assess, among other things, the following:

- a) impacts (financial, reputation, business continuity, etc.), if the service provider fails to comply with the terms and conditions of a contract in the expected manner and volume;
- b) potential loss or damage to be incurred by the bank and other parties/persons, if the service provider fails to comply with the terms and conditions of a contract in the expected manner and volume;
- c) the ability to comply with supervisory and regulatory requirements (taking into account possible changes in these requirements) and the consequence for the bank of the service provider failing to meet these requirements;
- d) the consumption of financial resources and time in the case of a need to replace a service provider or reinstate the provision of the service in the responsibility of the bank (business continuity management);
- e) the need for, and the terms and conditions of, carrying out due diligence of the service provider, and ensuring business continuity management;
- f) issues relating to the ownership right in physical and intellectual property (e.g. hardware and software, licenses, documentation concerning systems and processes).

68. The FSC will not agree to any of the following functions being outsourced:

- (a) compliance or a core management function;
- (b) any activity, if the outsourcing of that activity would

¹ Outsourcing means the assignment of certain activities necessary for carrying out the day-to-day business of a bank (e.g. development and management of information technology, cash management, administration activities, personnel management, real estate management, transportation) to third persons.

- (i) impair the FSC's ability to supervise the licensee; or
- (ii) affect the rights of a client against the licensee, including the right to obtain legal redress.

In this context, the following are considered to be "core management functions":

- (a) the setting and approval of the licensee's risk management and other strategies;
- (b) the oversight of the licensee's policies, systems and controls; and
- (c) the responsibility for the delivery of services to the licensee's clients.

69. Outsourcing arrangements should be based on contracts containing explicit terms and conditions that ensure a clear allocation of rights, obligations and responsibilities between external service providers and the outsourcing bank. The rights and obligations of the parties to such a contract should be clearly defined, understandable and applicable. The terms and conditions of the contract should, as a general rule:

- a) clearly specify all material aspects of the outsourcing arrangement, including
 - (i) the activities to be outsourced;
 - (ii) the rights and responsibilities of the parties; and
 - (iii) the protection by the service provider of confidential information relating to the licensee or its clients;
- (b) give the licensee and, if relevant, its auditor, access to all documents and information relevant to the outsourced activity, at all times;
- (c) provide for the orderly termination of the outsourcing arrangement, and
- (d) allow access to the service provider by the FSC.

A licensee should also establish and maintain a contingency plan for each outsourcing agreement into which it enters.

70. Before entering into any arrangement for the outsourcing of activities to a service provider, the Directors should undertake appropriate due diligence with respect to the service provider to enable assessment of –

- (a) the service provider's capacity and ability to undertake the outsourced activities; and
- (b) the risks associated with outsourcing the proposed activities to the service provider.

71. Outsourcing activities can reduce the risks of a bank by transferring certain activities to persons with greater expertise and opportunities to carry out these activities and to manage the risks associated with the activities. However, the use of external service providers does not diminish the responsibility of the Board or senior

management of a bank to ensure that the outsourced services are provided in a safe manner (including the protection of customer data) and in compliance with applicable laws.

BUSINESS CONTINUITY MANAGEMENT²

72. For reasons that may be beyond the control of a bank, circumstances can occur that result in the inability of the bank to fulfill some or all of its business obligations (including liquidity), particularly where the bank's physical, telecommunications, or information technology infrastructures have been damaged or made inaccessible. This can, in turn, result in significant financial losses to the bank, as well as broader disruptions to the financial system. Therefore, a bank should establish disaster recovery and business continuity plans that take into account different types of plausible scenarios to which the bank may be vulnerable, commensurate with the size and complexity of the bank's operations.

73. With a view to the implementation of the disaster recovery and business continuity plan, a bank should, among other things:

- a) appoint persons responsible for taking control of crisis management and business resumption;
- b) review its succession plans and 'key person' risk exposure;
- c) carry out relevant training programs, including communication with the media and public;
- d) create and supply a crisis management site;
- e) enter into preliminary agreements with possible internal and external persons and external service providers;
- f) create alternative options for recording and backing up electronic data;
- g) introduce the plan within the bank and carry out awareness/readiness checks;
- h) prepare communication with all interested parties.

74. Particular attention should be paid to the ability to restore the electronic data that is necessary for business resumption. Where the copies of such data are maintained at an off-site facility, or where the operations of a bank must be relocated to a new site, care should be taken that these sites are at an adequate distance from the impacted operations to minimize the risk that both original and

² Business continuity management comprises activities that are designed to improve the ability of a bank to respond to business interruptions and to restore its key activities, systems and process within an agreed period of time, while maintaining the critical activities of the bank.

back-up data and both primary and back-up facilities will be unavailable simultaneously.

75. The bank should periodically review its disaster recovery and business continuity plan to ensure that it is consistent with the bank's current operations and business strategies. Moreover, such a plan should be tested periodically to ensure that the bank is able to execute the plan in the actual event of a business disruption.

Conclusion

76. In the course of its on-site examinations the FSC will look for a Board approved operational risk policy, outsourcing policy and contractual documents and a Business Continuity Plan that includes a Disaster Recovery Plan and discuss implementation of these policies with bank management.

Date of Effect

77. This Prudential Statement takes effect from 1 December 2009

Financial Supervisory Commission

21 October 2009

