CENTRAL BANK OF SOLOMON ISLANDS

Financial System Regulations Department

Prudential Standard No. 3
Operational Risk Management

TABLE OF CONTENTS

1. Introduction

General stipulations

1. The requirements in this Prudential Standard are specified pursuant to section 8 of the Financial Institutions Act 1998, as amended.

2. Part III of the Financial Institutions Act 1998 states that in determining whether or not a bank carries on its business in a prudent manner, the Central Bank of the Solomon Islands (CBSI) shall have regard to internal controls and risk management and such other matters as the CBSI considers relevant. The CBSI will have regard to the application of this Prudential Standard in determining whether or not a bank carries on its business in a prudent manner.

Objectives

3. This Prudential Standard addresses the operational risk inherent in all banking products, activities, processes and systems. The effective management of operational risk is a fundamental element of a bank's risk management.

4. This Prudential Standard establishes the CBSI's minimum requirements for the management of operational risk by a bank.

5. The ultimate responsibility for the comprehensive and effective management of operational risk rests with the Board of Directors of a bank. It is the responsibility of the Board of Directors, and Senior Management of a bank to adopt and implement, on a continuing basis, a risk management framework covering the operational risks incurred by the bank. This operational risk management framework, and the policies and processes it contains, must be approved by the Board of Directors, and must provide, as a minimum, for the bank to-

    - have an operational risk appetite statement that articulates the nature, types, and levels of operational risk that the bank is willing to assume;
    - implement and apply governance, structures, processes and systems for identifying, assessing, measuring, monitoring, reporting, and controlling or mitigating, on a prudent basis, operational risks encountered by a bank;
    - establish, and apply, prudent limits and thresholds on operational risks;
    - ensure the bank meets, at all times, all the minimum requirements in this Prudential Standard applicable to a bank's management of operational risk.

Application

6. This Prudential Standard is applicable to all banks licensed by the CBSI under the Financial Institutions Act 1998. The CBSI may by order direct a bank to take specific actions with regards its operational risk management framework and its management of operational risk.

7. A bank must inform the CBSI when it becomes aware of a significant, or material deviation from its operational risk management framework, or it becomes aware that the framework does not adequately address any material operational risk.

8. Where a bank, or another entity, is head of a consolidated group it must, where relevant, comply with the requirements of this Prudential Standard:

   (a) in its own capacity;

   (b) by ensuring that the requirements in this Prudential Standard are applied appropriately by each entity throughout the consolidated group of which the bank is a member, including in relation to entities that are not regulated by the CBSI; and

   (c) on a group basis.

9. Where there is a reference to a Board of Directors in this Prudential Standard, for a consolidated group, should one exist, it refers to a Board of Directors of:

   (a) the bank;

   (b) any other regulated entity, if any, in the consolidated group; and, as well,

   (c) the head of the consolidated group, if it is not the bank.

Enforcement and corrective measures

10. A financial institution which fails to comply with the requirements contained in this Prudential Standard or submits reports to the CBSI which are materially inaccurate will be considered as following unsound and unsafe practices as provided in Section 16 (1) (a) of the Act.

11. The CBSI may pursue any or all corrective measures as provided in Section 16 of the Act to enforce the provisions of this PS including:

   (a) issuance of an order to cease and desist from the unsound and unsafe practices; and

   (b) action to replace or strengthen the management of the financial institution.

References

12. This Prudential Standard should be specifically applied in conjunction with the following related Prudential Standards:

   (a) Prudential Standard on Governance (No. 1)

   (b) Prudential Standard Risk Management (No. 2)

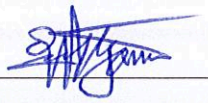
   (c) Prudential Standard on Business Continuity Management (No.4)

   (d) Prudential Standard on Outsourcing of bank activities (No. 6)

Effective Date

The effective date of this Prudential Standard is 30th December 2024.

Issued this 28th day of June, 2024



Luke Forau, PhD, Governor

Central Bank of Solomon Islands

2. Definitions

13. Terms used within this Prudential Standard are as defined in the "Act", and as defined below, or as reasonably "implied by context. Terms are as follows-

(a) **"Act"** - the Financial Institutions Act 1998, as amended.

(b) **"Board of Directors (Board)"** means the highest body of authority in a bank responsible for strategically guiding the bank, effectively monitoring management, and properly accounting to shareholders. It is the body that supervises management.

(c) **"CBSI"** – Central Bank of the Solomon Islands

(d) **"Consolidated group"** – refers to a group of entities, if any, to which consolidated group requirements: are applied under the Capital Prudential Guideline or other Prudential Standards.

(e) **"Defense in depth"** – is a concept in which multiple layers of internal controls are placed within a business process to prevent, detect, or reduce the impact of a process breakdown in case any internal controls are compromised. When applying this concept, a bank should balance the strength of the embedded internal controls against the associated level of operational risk exposure.

(f) **"Directors" -** means members of the Board of a bank, whether permanent or alternate

(g) **"Disaster Recovery Plan"** means a documented, structured approach with instructions for responding to disastrous events.

(h) **"Foreign bank branch"**- means the branch of a (foreign) bank incorporated outside of the Solomon Islands which is licensed as a bank in the Solomon Islands under the "Act".

(i) **"Bank"**- has the meaning in the "Act".

(j) "**Information and communication technology"** - refers to the underlying physical and logical design of information technology and communication systems, the individual hardware and software components, data and the operating environments.

(k) **"Legal risk"**- includes, but is not limited to, exposure to fines, penalties or punitive damages resulting from supervisory actions as well as ordinary damages in civil litigation, related legal costs and private settlements.

(l) **"Operational risk"** - means the loss resulting from inadequate or failed internal processes, people, and systems or from external events. This definition includes legal risk but excludes strategic and reputational risk. Operational risk is inherent in all products, activities, processes and systems of a bank.

(m) **"Operational risk event"** - defined as an unintended outcome resulting from operational risk. It includes actual and potential operational losses and gains, as well as near misses (i.e., where a bank did not experience an explicit loss or gain from an operational risk event).

(n) **"Operational risk culture"**- means the combined set of individual and corporate values, competencies and behavior that determines a bank's commitment to and styles of operational risk management.

(o) **"Operational Risk Management"-** encompasses the process of identifying and assessing the inherent operational risk of the bank, measuring exposures to those risks (where possible), monitoring risk exposures on an on-going basis, takings steps to control or mitigate risk exposures and reporting to senior management, the Board of the bank, and the CBSI (as required) on the bank's operational risk exposures.

(p) Operational risk management also encompasses the recognition and assessment of capital (and liquidity, as appropriate) needs arising from the operational risk faced by the bank and ensuring that effective capital (and liquidity) planning and monitoring are in place, on an on-going basis, to meet the identified needs.

(q) **"Operational risk management framework"** – means the organizational structures, policies and strategies, processes, procedures and systems used in identifying, assessing, measuring, monitoring, controlling, mitigating and reporting operational risk.

(r) **"Operational risk appetite statement"**- is a high-level written determination by the Board of a bank as to how much operational risk the bank is willing to accept taking into account the risk/return attributes (i.e., its risk appetite or tolerance). It is often taken as a forward-looking view of risk acceptance and typically involves the establishment of limits and thresholds on the level, or amount, or type of operational risk an entity is willing to accept.

(s) **"Person"** – means an individual or entity.

(t) **"Senior Management"** – includes permanent and contracted persons occupying or acting in the role of an executive officer of the bank. They include, but are not limited to persons-

- in the capacity of, or acting in the function of chief executive officers, general or senior managers, or
- individuals holding positions whose conduct have a significant impact on the sound and prudent management of the bank's day-to-day administration or operations or persons employed or contracted by the bank that can make a policy decision.

3. Prudential requirements

Governance

14. A bank is required to have a clear, effective and robust governance structure for operational risk with a well-defined, transparent and consistent lines of responsibility.

15. The governance applied to the operational risk of a bank should be commensurate with the structure, nature, size, size and complexity of the operations of the bank.

Role of board of directors and senior management

16. Whilst the ultimate responsibility for operational risk management resides with the Board of a bank, it is essential that:

    (a) all operational risk management roles and responsibilities must be clearly understood and executed. This includes that all staff of the bank, whatever their level, clearly understand their individual roles, responsibilities, authority to act, and accountability in the operational risk management process; and

    (b) a proactive risk culture is created to support the identification and reporting of operational risk related issues to relevant personnel in the bank.

17. The Board of Directors, and the Senior Management of a bank must ensure a strong risk culture exists throughout the whole of the bank. Such culture must support and provide appropriate standards and incentives to professional and responsible behavior. This should include a code of conduct, or an ethics policy, endorsed and clearly supported, and compliance monitored, by the Board of Directors and Senior Management, that sets expectations for integrity and ethical values of the highest standard and which identifies acceptable business practices and prohibited conflicts of behavior.

18. The Board is ultimately responsible for the sound management of a bank's operational risk and must ensure the bank has a robust operational risk management framework to manage this risk accordingly.

19. The Board of a bank is required to:

    (a) recognise operational risk as a distinct risk category;

    (b) recognise the major operational risks inherent in its business and understand the risk management framework for this;

    (c) receive reports that enable it to understand the overall operational risk profile of the bank and focus on the material and strategic implications;

    (d) approve a structure for the management of operational risk within the bank including the assigned authority, responsibility, accountability and reporting relationship developed by Senior Management. This includes designating the person or persons in the bank responsible for the day-to-day oversight of operational risk management in the bank including:

        (i) the effective implementation of approved policies and procedures for the management of operational risk in the bank;

        (ii) reliable monitoring and reporting of operational risk events (including losses or risky actions); and

        (iii) application of internal controls and risk mitigation, including compliance with limits and thresholds;

    (e) ensure, in conjunction with Senior Management, that adequate resources are allocated to ensure the continuous development and implementation of the required level of management of the bank's operational risk; and

(f) ensure that Senior Management, and through them, the bank as a whole, is actively monitoring the implementation, effectiveness and compliance with the banks operational risk management framework, including the Board approved operational risk appetite statement.

20. The Board of a bank must establish an operational risk appetite statement that is succinct, clear, and:

(a) articulates the nature, types and levels of operational risk (including losses arising from operational risk) that the bank is willing to assume; and

(b) includes measurable components (limits and thresholds) on the level of operational risk considered acceptable by the bank. Such limits and thresholds will form the foundation for indicating the level of operational risk events, breaches, near misses or cumulative patterns which are considered necessary for escalation for the attention of Senior Management and the Board of the bank.

21. In formulating (and reviewing) an operational risk statement, the Board of a bank would need to have regard to, but not limited to:

(a) changes in the external environment;

(b) material increases or decreases in the bank's business or activity volumes (and associated operational risks) overall, and by type;

(c) the operational risk impact of new products, activities, processes or systems implanted or proposed to be implanted by the bank;

(d) developments in best practice for measuring, controlling and mitigating, and reporting operational risk and whether the bank has availed itself of such practice;

(e) the quality of the control environment within the bank for the management of operational risk. This includes the adequacy of the identification and assessment of operational risks faced by the bank;

(f) the effectiveness of the risk management or mitigation strategies applied by or proposed to be applied by the bank;

(g) the bank's experience with operational risk events, including the type and amount of operational risk losses incurred; and

(h) the frequency, volume or nature of risk appetite limit/threshold breaches.,

22. The Board of a bank must ensure that a bank has a robust operational risk management framework to manage the operational risk of the bank in accordance with the operational risk appetite statement by the Board of the bank.

23. The Board of a bank must approve and oversee the implementation of the operational risk framework of the bank. The operational risk management framework must be fully integrated with the bank's overall risk management process.

24. The Board must ensure it receives regular and adequate reporting, and information, on operational risk and management of the bank. This includes, but is not limited to:

(a) pertinent information on current and emerging operational risk exposures and vulnerabilities of the bank. This includes adherence to the operational risk appetite statement and material breaches of limits and the status of remediation of breaches;

(b) the effectiveness of the operational risk management framework in the bank; and

(c) the outcome of independent reviews by internal audit or other qualified persons on the application, adequacy and effectiveness of operational risk appetites and the operational risk management framework.

25. The Board must satisfy itself on a regular basis with the level of operational risk faced by the bank and the adequacy, appropriateness and effectiveness management of this risk.

26. The operational risk appetite statement, and operational risk management framework approved by the Board of the bank, and their implementation must be subject to regular (at least annual) review by the Board.

27. A Board may delegate its powers, functions or duties to a Board committee relating to operational risk. The committee must have a clearly defined responsibilities, operational risk loss thresholds for reporting to the Board and performance obligations. Notwithstanding such delegation, the Board retains full responsibility for ensuring compliance with the requirements in this Prudential Standard.

28. For foreign bank branches, the Country Head for a branch is responsible, in the first instance, with satisfying the obligations placed on the Board of a bank in this Prudential Standard with respect to the implementation and application of an operational risk management framework covering the foreign bank branch's operations in the Solomon Islands. In addition, the Board of Directors of the bank shall be ultimately responsible for ensuring compliance with the requirements of this standard.

29. While the Country Head may not determine the risk appetite for the foreign bank branch's operations in the Solomon Islands, nevertheless, it is the responsibility of the Country Head to ensure that an operational risk appetite statement of the foreign bank has been applied in respect of the operational risk of the branch's operations in the Solomon Islands. This would include application of limits and thresholds specific to the foreign bank branch's operational risk in the Solomon Islands.

Senior management

30. Senior Management of a bank is responsible for the translation of the operational risk appetite statement and operational risk management framework approved by the Board of the bank into specific policies and procedures that can be implemented, and verified within different business units of the bank.

31. Senior Management is responsible for ensuring the operational risk appetite statement and operational risk management framework approved by the Board is implemented consistently and effectively throughout the bank.

32. Senior Management of a bank is required to:

(a) ensure the identification and assessment of all the operational risk inherent in all the existing, and any new, products, activities, processes and systems of the bank and that such risks are recognised and well understood within the bank;

(b) develop, implement and verify detailed policies and procedures for managing operational risk in all business activities and across all processes and systems;

(c) determine the structure, responsibilities and controls for managing operational risk. This should ensure business and functional lines are also responsible for the identification, assessment, mitigation and review of operational risk for specific products, activities, processes and systems within their purview;

(d) ensure that the bank has adequate internal controls to safeguard the integrity of its operational risk management framework;

(e) upon approval of the Board, clearly assign authority, responsibility and reporting relationship in the bank to facilitate decision-making, reporting and ensure accountability;

(f) ensure that the banks 's activities, including operational risk management roles are conducted by staff with the necessary experience, technical capabilities and access to resources;

(g) ensure the appropriate level of operational risk training is available throughout the bank and that training is provided should reflect the seniority, role and responsibilities of the individuals for whom it is intended;

(h) ensure adequate resources are available to support all staff of the bank in discharging their responsibilities for operational risk management;

(i) communicate clearly the operational risk management policy to staff across all risk areas within the bank that incur operational risks, notably material operational risks;

(j) ensure staff responsible for the management of operational risk, coordinate and communicate effectively with-

- staff in the bank responsible for managing credit, market, liquidity and other risks; and

- those staff within the bank who have responsibility for procuring risk mitigation services (e.g., insurance risk transfers);

(k) specify the scope, manner and frequency of reporting for various recipients (such as the Board, Senior Management and any risk and credit committees), and specify the persons responsible for preparing the reports; and

(l) closely monitor internal and external developments that may present challenges for managing the bank's operational risk, so that appropriate and timely changes to the operational risk management framework can be made as needed.

33. The Senior management of a bank must:

(a) continuously review information on the bank's operational risk developments and report to the Board of the bank on a regular basis;

(b) notify the Board the bank in a timely manner of material changes or exceptions from established policies and procedures that could affect the operational risk management framework;

(c) promptly notify the Board of material breaches of limits and thresholds applied to operational risk; and

(d) inform the Board (and appropriate Senior Management in the head office of a foreign bank branch) of any questions, or criticism, by the CBSI with respect to-

- material aspects of the bank's management of operational risk; or

- the adequacy or effectiveness of the bank's operational risk management framework.

Risk management process

34. Risk management encompasses the establishment of policies, and procedures providing for identifying risks to a bank, measuring exposures to those risks (where possible), ensuring effective monitoring and reporting of risk exposures, and implementing controls or mitigation of operational risk exposures.

35. The effective management of the operational risk inherent in a bank necessitates that the management of operational risk should be a fundamental element of a bank's overall risk management program. Operational risk should be governed by its own policy or be sufficiently prominent in an overall risk management framework to assure the CBSI of its inclusion.

36. The management of operational risk must also be fully integrated into a bank's overall risk management processes. This includes, where appropriate, coordinated with the management of other risks faced by the bank, and factored into capital, liquidity and other of the bank's risk management assessment and planning processes.

Operational Risk Management Framework

37. A bank must establish and implement, on a continuing basis, a sound, appropriate, comprehensive and effective operational risk management framework approved by the Board of the bank.

38. A bank's operational risk management framework must be clearly documented. A copy of the framework must be made available to the CBSI, on request. Any material changes to the framework must be promptly notified to the CBSI.

39. A foreign bank branch may rely in part, or in full, on an operational risk management framework established and applied by the head office of the foreign bank. This, provided that the foreign bank branch can satisfy the CBSI the requirements, or those part of the requirements, in the operational risk management framework applied to operational risk of the foreign bank branch incurred in the Solomon Islands are equivalent to or more stringent than the requirements set out in this Prudential Standard. Reliance by a foreign bank branch on application of an operational risk management framework applied by head office of the foreign bank, in full or part, does not excuse a foreign bank branch from compliance with the requirements in this Prudential Standard.

Policies and strategies

40. The starting point for an operational risk management framework is the development and implementation of Board approved risk management policies / strategies covering the bank's management of its operational risk. This includes critically the establishment of a risk appetite statement for operational risk.

Operational risk appetite statement

41. A bank's operational risk framework must reflect the operational risk appetite statement approved by the Board. This operational risk appetite defines the amount of operational risk that the Board of the bank is willing to accept in the bank in order for it to meet its strategic objectives.

42. A bank's operational risk management framework must contain a clear description of risk limits and risk impact thresholds that flow from the bank's operational risk appetite statement, and describe the bank's approach to establishing and monitoring of the limits and thresholds.

43. The content and scope of the policies and strategies applied in a bank's operational risk management framework must:

    (a) be commensurate with the risk appetite adopted by the bank;

    (b) be appropriately designed for the size, nature, complexity, volume and scale of risk and activity of the bank's products and activities and the operational risk profile they generate;

    (c) reflect the internal and external environment within which the bank's activities take place; and

    (d) apply appropriate and prudent risk management standards and objectives in relation to operational risk across all key underlying business and support processes of the bank.

44. The policies and strategies forming the basis of a bank's operational risk management framework must also:

    (a) be readily understood and auditable;

    (b) be clearly communicated to all employees on a regular basis, to ensure that they are fully understood by the people responsible for managing operational risks; and awareness levels are maintained and are consistently applied;

    (c) facilitate the monitoring, measurement and management of operational risk of the bank;

    (d) provide for the ongoing development of new policies and strategies reflecting the experiences of the bank, changes in its products and activities, and future external developments which impact the bank's operational risk profile;

    (e) identify the structure to be applied for the management of operational risk within the bank, and the roles of persons withing that structure and their duties, responsibilities along with their level of authority and accountability in the management of the bank's operational risk;

    (f) provide for regular review and update of policies and strategies to ensure they continue to appropriate and reflect the environment within which the bank operates;

    (g) cover at least the following functions, as they exist, or applied in the bank; Human Resources, Internal Controls, Compliance, Internal Audit, Administration, Outsourcing, Information Technology, Business Continuity Planning, Internal Fraud, External Fraud, New Product Development and Change Management.

Identification of operational risk

45. A bank's operational risk framework must provide for sound approaches to operational risk identification, measurement and assessment that utilizes appropriate operational risk management tools. Risk identification and assessment are a fundamental characteristics of an effective operational risk management system.

46. A bank's operational risk management framework must provide a description of risk assessment and management tools to be used, and when and how they are to be used. The identification of operational risks should ensure the full spectrum of operational risks facing the bank, both actual and potential, are identified, assessed and appropriately measured.

47. The operational risk identification process provided in a bank's operational risk management framework must consider:

    (a) the full spectrum of current and potential operational risks applicable to the bank;

    (b) the potential causes of the operational risk;

    (c) the existing internal and external environment in which the bank operates;

    (d) the bank's strategic objectives;

    (e) the products and activities the bank provides or undertake;

    (f) the bank's structure and the level and quality of resources applied within a bank to the management of operational risk

    (g) the bank's unique circumstances; and

    (h) the internal and external environmental changes that may impact the bank and the pace of changes.

48. The internal environment includes a bank's structure, activities, quality of staff, organisational changes, employee turnover and its products and services. External environment includes technological advances, changes in industry and other market information that affects, or may affect, the achievement of the banks 's objectives. It would include, in particular, environmental changes (e.g., possible impact of global warming) and the potential for natural disasters (e.g., cyclones, earthquakes etc.) and their impact.

49. The process for the identification and assessment of operational risk can include, but is not limited to, the use of key risk indicators, risk and compliance registers and, risk maps.

Controls and risk mitigation

50. A bank's operational risk framework must include approved control (e.g., limits and thresholds) and risk mitigation processes and strategies that effectively address all identified operational risk in line with the operational risk appetite set by the Board.

51. A bank must be able to demonstrate that the controls and risk mitigation processes and strategies adopted in its operational risk management framework can contain operational risk exposures of the bank within the operational risk appetite set by the Board.

52. A bank's operational risk management framework must provide for a regular assessment and verification of the bank's operational risk exposures and a process for affirming that the risk

mitigation strategies and responses remain appropriate, effective and have value. For example, careful consideration needs to be given to the extent to which risk mitigation tools such as insurance truly reduce risk, transfer the risk to another business sector or area, or create a new risk (eg counterparty risk).

53. When devising risk mitigation strategies, a bank must consider the impact of the mitigation strategies on other risks faced by the bank, and whether the strategies adopted could introduce new risks to the bank or could create unintended effects on risk-taking incentives or on business and operational performance. These implications must be clearly identified and effectively addressed as part of the bank's overall risk management framework

54. A key element of the application of control and risk mitigation strategies is the inclusion and application, as part of a bank's operational risk management framework of processes to ensure that controls and risk mitigation strategies have been effectively implemented. These processes include-

(a) identification of when controls (e.g., limits and thresholds) and risk mitigation strategies have been, or may potentially, be breached or not be fully implemented as required;

(b) the how and timing of when breaches and failure to implement were discovered;

(c) the level of breaches and failure to implement;

(d) reasons for breaching or failure to implement;

(e) whether any breaches or failure to implement were authorised, the timing of when authorisation was granted, and by whom any authorisation was given and the level of authority applicable to any approval process; and

(f) the application and escalation of notification and approval for actual or potential breaches and failure to implement.

New products and activities

55. A bank's operational risk management framework must ensure that the bank has in place a process for review and approval of new products, activities, processes and systems. The review and approval process must consider-

(a) inherent risks in the new product, service or activity;

(b) the impact of new products, activities, processes and systems changes on the bank's operational risk profile and operational risk appetite, including the risk of existing products and activities;

(c) the necessary controls, risk management processes and metrics, and risk mitigation strategies required to identify, measure, assess, monitor, report and manage the operational risk and impact of the new products, processes and systems; and

(d) any changes to relevant risk limits and thresholds.

56. It is vital that a bank's operational risk management framework ensures operational risk management controls and infrastructure remains appropriate and keeps pace with rate of growth or changes in products, activities, processes and systems.

57. A bank's operational risk management framework should ensure close monitoring of the implementation of new products, activities, processes and systems to identify any material differences to expected operational risk profiles and to manage unexpected risk outcomes.

Governance structures

58. A bank's operational risk management framework must contain a defined and appropriate governance structures as it relates to operational risk management, including approval, accountability and reporting lines. The structure should define the role, responsibilities, and accountability of the Board and Senior Management, personnel directly engaged in operational risk management; and all other staff of the bank, as appropriate for the identification, reporting, controlling, mitigating and otherwise managing operational risk within the bank.

59. Personnel engaged within a bank in operational risk management must have appropriate levels of expertise and experience. To this end, the bank's operational risk management framework must include a register of Senior Management and other personnel directly engaged in the management of operational risk within the bank, and their expertise and experience. Such a register must be regularly updated following changes. This register must be provided to the CBSI, upon request.

60. A bank must ensure personnel responsible for monitoring and enforcing compliance with the bank's operational risk policies should have independent authority from the areas they oversee.

Monitoring and reporting

61. A bank's operational risk management framework must ensure-

(a) the collection of information on operational risk;

(b) the provision of regular formal reporting on the existing operational risk of the bank; as well as

(c) the collection and provision of information on new or emerging operational risk.

62. Information (including operational loss data) collected and provided must be complete, accurate, reliable, timely, consistent and actionable, including all information relevant to decision-making in a bank's management of its operational risk.

63. A bank's operational risk framework must provide documented procedures for the identification, collection and the reporting of information on the operational risks encountered by the bank.

64. The information on operational risk collected and reported by a bank must be provided to business lines, Senior Management, and the Board, as applicable. The information must enable the Board and Senior Management to be assured of –

(a) the bank's compliance with the policies, strategies, controls and risk mitigation provided for in the bank's operational risk management framework; and, most importantly,

(b) the compliance by the bank with laws, regulations and prudential requirements to which it is subject, including compliance with the requirements in this Prudential Standard.

65. Information to be reported must include-

(a) the current operational risk profile, emerging trends of key operational risk indicators and the direction of operational risks over a defined horizon (e.g. over the next three months);

(b) the classification of identified operational risk exposures by operational category within the bank's established operational risk taxonomy;

(c) whether operational risk exposures identified are actual, potential or is a near miss event;

(d) the status of mitigation action plans for (material) operational risks;

(e) breaches of operational risk limits and thresholds, in particular, those resulting in the bank's enterprise-wide operational risk levels being higher than the approved risk appetite;

(f) sign-offs and approvals for breaches of limits and thresholds;

(g) observations of operational risk management deficiencies by the operational risk management function, internal audit or the CBSI;

(h) significant operational risk events, control failures and losses that have occurred; and details of the corrective actions, if any, implemented within the bank to address (and prevent) control failures and operational risk losses which may have been generated; and

(i) lessons learnt from relevant external loss events and internal assessments of the probability and potential impact of similar events occurring in the bank.

66. The scope, context and level of granularity of operational risk reporting must be appropriately tailored to the needs of the different groups of users of the reports within a bank. It needs to relevant, manageable in scope and volume. For example, detailed operational risk information specific to activities and operations of the business and functional lines is appropriate and useful to the business and functional line management, whereas a high-level overview of the overall operational risk profile of the bank and executive summaries of significant enterprise-level operational risks would be more beneficial to facilitate decision-making by the Board and Senior Management.

67. Information must be provided in a timely manner to enable timely management and Board responses to developments in a bank's operational risk profile and the management of its operational risk. Reporting frequency must reflect the level of operational risks involved, as well as the pace and nature of changes in the business and operating environment of the bank.

68. To meet the requirements for provision of information for the management of operational risk, a bank must have a robust management information system (MIS) that produces data and other information required for adequately assessing the operational risk exposure of the bank for all operational risk components.

69. A bank must have in place a structure and process for ensuring that the reporting of information -

(a) fully reflects any identified problem areas in operational risk and prompts timely and corrective action on outstanding issues; and

(b) is distributed to appropriate levels of management to all areas of the bank to which the information is relevant (including the Board) of the bank, as appropriate.

70. A bank's operational risk management framework must provide that the Board and Senior Management are able to respond appropriately, and promptly, to information contained in operational risk management reporting to them. In addition, arrangements for the reporting of information must include escalation procedures for reporting key operational risk issues to Senior Management and the Board to facilitate action between reporting cycles, if required.

71. A bank must provide the CBSI with copies of internal information collected and reported on operational risk, if requested. Reports generated for the CBSI whether in the normal course of reporting to the CBSI, or upon request from the CBSI, should be advised to the Board, and made available to the Board, at its discretion.

Integration of risk management

72. A bank's operational risk management framework must ensure:

(a) the bank's processes for managing the components of operational risk apply a comprehensive and consistent approach to identify and profile operational risks across all products and activities in which the bank offers or engages; and

(b) the operational risk management framework is well integrated with other risk management processes of the bank.

Review of operational risk management framework

73. A bank's operational risk management framework (including, but not limited to policies and strategies, controls and risk mitigation, reporting processes, breaches of controls and follow up actions) must be subject to regular (at least annual) effective and comprehensive independent review. In most cases, the independent reviews could be facilitated by the bank's internal audit function but may require the engagement of independent qualified persons outside of this function.

74. The review of a bank's operational risk management framework must incorporate a formal review by the Board each year of its appropriate risk appetite statement (and the policies and strategies which flow from this into the bank's operational risk management framework) to ensure that it is updated in line with the bank's activities, products, management processes, staff capacity, risk profile and future plans.

75. Reports relating to reviews of a bank's operational risk management framework, its internal controls and other aspects of its overall risk management must go to the Board or its audit committee or other committees, as appropriate. The Board or committees must formally respond to conclusions, recommendation or suggestions for action or improvement in the reviews along with reasons why recommendations or suggested actions are not acted upon, or partially acted upon. A copy of the reviews and responses must be provided to the CBSI, upon request.

76. A bank, at the request of the CBSI, must engage at the bank's expense, with the approval of the CBSI, either the bank's external auditor, or an appropriate external expert, to review and

provide an assessment to the CBSI of the bank's operational risk management framework. The external auditor of the bank cannot undertake such a review should the external auditor also provide the internal audit function for the bank.

Key Operational Risk Management Matters

(i) Independent operational risk management function

77. A bank should, at a minimum, have in place an independent operational risk management function. The role of this function would be design, implement and continuously develop the bank's operational risk management framework and to assist Senior Management (and the Board) in meeting their responsibility for understanding and managing operational risk.

78. The independent operational risk management function should at a minimum:

(a) establish, maintain and monitor compliance arrangements, including processes and procedures that ensure compliance with the operational risk management framework;

(b) define and document all roles, responsibilities and functions pertaining to the management of operational risk;

(c) ensure consistent status reporting to the Board and Senior Management;

(d) design and implement a monitoring and reporting system for operational risk;

(e) identify and monitor emerging trends and issues; and

(f) ensure consistent liaison with internal and external audit.

79. The CBSI may consider an approach from a bank to incorporate the operational risk management function as part of a broader risk management function within the bank. Such a function may undertake and have responsibility for overall risk management within the bank beyond just operational risk management. The CBSI's agreement to such a sharing of risk management functions within the bank involving operational risk management will have regard to, but not limited to:

(a) the size of the bank; and the volume and range of products and activities it offers and undertakes;

(b) trends in the bank's products and activities which it offers and undertakes, and the bank's business plans impacting its future product offerings and activities;

(c) the levels of operational risk identified with the products and activities the bank offers or is engaged in, or plans to offer or become engage in the foreseeable future;

(d) the expertise, experience, and level of personnel who might be engaged in operational risk management functions as part of their broader risk management responsibilities;

(e) the nature, scale and scope of the bank's operational risk management framework; and

(f) the performance of the bank's operational risk management framework, including levels of operational losses incurred, breaches of limits and thresholds or any other failings with the operation of the framework.

80. The CBSI will need to be satisfied that the functions required to be performed by an independent operational risk management function (refer Paragraph 75 of this Prudential Standard) are being undertaken, albeit not in an independent operational risk management function itself.

81. In the case of foreign bank branches that are not considered systemically important for Solomon Islands, on receipt of a written request from a bank, CBSI may agree to waive the requirement of having an independent operational risk management function in Solomon Islands. Where the CBSI agrees to waive the need for a bank to have an independent operational risk management function, such a waiver may be subject to terms and conditions especially the quality of operational risk management of the branch and its operational loss experience at least during last five years. Breaches of terms of conditions and conditions may cause any waiver granted by the CBSI to be void. Agreement by the CBSI to waive the need for an independent operational risk management function will be subject to review by the CBSI and any waiver may be withdrawn following a review.

(ii) Internal controls

82. An essential part of the management of its operational risk, is the implementation by a bank of a set of robust and logical internal controls. The internal controls must be adequate for the size and complexity of the banks business and the risk profile of the bank. This includes operational risk.

83. Internal controls must support the effective control of operational risks at multiple stages and layers within the operations of the bank business process to provide adequate defence in depth to any breakdown in controls at any stage or layer of a bank's operations.

84. Internal controls which a bank would implement in addressing the management of its operational risk would include, but not be limited to:

(a) clearly established authorities and/or processes for approval. A system of graduated approvals must be provided having regard to the type, size, complexity or speed of the business being undertaken by the bank with stronger controls required as operational risks increase;

(b) clearly defined responsibilities for reporting across all personnel. A bank must ensure there are no gaps in reporting lines that may enable the concealment of unauthorised actions and material errors or losses in relation to operational risk or other risks;

(c) close monitoring of adherence to assigned limits or thresholds. This would incorporate analysis of approved exceptions to limits, management overrides and other deviations from policies and strategies governing operational risk management. As well, it would capture the review of the identification, treatment and resolution of non-compliance with limits, thresholds or other parts of the bank's operational; risk management framework

(d) safeguards for access to, and use of, the bank's assets and records;

(e) appropriate staffing level and training to maintain expertise;

(f) ongoing processes to identify business lines or products where measured and returns (and reported levels of operational risk) appear to be out of line with reasonable expectations;

(g) regular verification and reconciliation of transactions and accounts; and

(h) minimize areas of potential conflict in management of operational risk, and ensure critical areas of operations are subject to appropriate segregation of duties, dual control and independent monitoring.

85. The internal control environment of a bank must be subject to appropriate independent internal audit review to test adherence to these controls as well as applicable laws, regulations and any supervisory requirements.

86. A bank must, specifically, monitor and regularly evaluate its internal control systems to ensure that they are operating effectively and take account of changes in internal and external conditions affecting its management of its operational risks. Enhancements must be made by the banks to internal controls to address any identified gaps and to maintain the effectiveness of the controls.

87. An important part of internal controls is the on-going monitoring and enforcement of compliance with a bank's operational risk management framework. As part of its internal controls addressing operational risk management, a bank must -

(a) affirm in the operational risk management framework the importance of compliance;

(b) clearly designate the persons or persons with the role and responsibility for monitoring, reporting and enforcement of compliance;

(c) ensure those undertaking compliance roles are equipped with the necessary skills, expertise, and experience to oversee compliance in line with the volume and complexity of the bank's products and activities. Persons undertaking compliance roles should be afforded the level of seniority commensurate with the importance of ensuring compliance; and

(d) ensure that adequate levels of advice and training on compliance requirements within the bank's operational risk framework, and on compliance with legal and regulatory requirements and standards, are provided to all relevant personnel within the bank.

88. Fraud represents a core element within the operational risks a bank may face, and therefore requiring particular attention with a bank's internal controls covering operational risk.

89. As part of its internal controls, a bank must-

(a) have in place proper financial accounting controls and adequate monitoring. It should include red flags that can quickly identify potentially fraudulent activities;

(b) ensure that regular management reports should cover not only amounts and types of fraud, but the trend analysis of the particular fraud; and

(c) ensure that staff are trained on the potential sources of fraud and the application of controls used in fraud risk management.

(iii) Internal audit

90. A bank must ensure internal audit oversight and review of its operational risk management framework. Internal audit coverage must be adequate to independently verify that the bank's operational risk management framework has been implemented as intended and is functioning effectively.

91. The internal audit function within a bank must supervise the implementation of operational risk management policies and independently evaluate new operational risk management policies, processes and specific procedures. Internal audit review would form part of the required review by a bank of how its operational risk management framework.

92. Internal audit must report to the Board, or via an audit committee or risk committee on the evaluation results of its reviews of a bank's operational risk management framework. Copies of internal audit reports, and the Board and committee responses to such reports must be provided to the CBSI, on request.

93. Internal auditors undertaking the review of a bank's operational risk management framework must have the appropriate expertise and experience to undertake this function, and must not have had involvement in the development, implementation or operation of the framework.

94. Internal audit coverage should include opinion on the overall appropriateness and adequacy of the bank's operational risk management framework and the associated governance processes across a bank. Internal audit should not simply be about testing compliance with Board approved policies and strategies, processes, controls and risk mitigation, and reporting for operational risk but also evaluate whether the operational risk management framework meets the bank's needs, and the CBSI's expectations contained in this Prudential Standard. For example, while internal audit should not be about setting risk appetite limits it should review the robustness of the process of how limits and thresholds are set, and why and how they need to be adjusted to changing circumstances affecting the operational risk profile of the bank and how the management of its operational risk is conducted.

(iv) Information and communication technology

95. A bank must ensure that its information and communications technology fully support and facilitates its operations.

96. Insofar as information and communication technology serves a significant, and increasingly more important, role in the conduct of a bank's operations, information and communication technology becomes a core source of the operational risk faced by a bank.

97. A bank must implement a robust management of its information and technology communication risks as part of its operational risk management framework. Such management must be appropriate to the significance of information and communication technology in its operations and the risks such technology may create.

98. A bank's management of its information and communication technology risks must reduce the bank's operational risk exposure to direct losses, legal claims, reputational damage, information and communication disruptions and misuse of technology in alignment with its operational risk appetite statement.

99. Information and communication technology risk management would specifically include:

(a) information and communication technology risk identification and assessment;

(b) information and communication technology risk mitigation measures consistent with the assessed risk level (e.g., cybersecurity, response and recovery programs, information and communication technology change management processes, information and communication technology incident management processes, including relevant information transmission to users on a timely basis); and

(c) monitoring of information and communication technology risk mitigation measures (including regular tests).

100. Information and communication technology risk management together with other complementing processes put in place by a bank must specifically be:

(a) reviewed on a regular basis for completeness against relevant industry standards and best practices as well as against evolving threats (e.g. cyber) and evolving or new technologies;

(b) regularly tested as part of a program to identify gaps against stated risk tolerance objectives and facilitate improvement of the information and communication technology risk identification, protection, detection and event management; and

(c) make use of actionable intelligence to continuously enhance the bank's situational awareness of its vulnerabilities to information and communication technology risks to facilitate effective decision making in its risk or change management.

(v) Business Continuity

101. A fundamental operational risk is that a bank for operational reasons cannot continue its business activities. Disruptions to a bank's business operations can result in significant financial losses to the bank, as well as broader disruptions to the financial system.

102. A bank as part of its operational risk management framework must specifically have in place Board approved business resiliency and continuity plans (including disaster recovery plans), commensurate with the nature, size and complexity of its operations, to ensure its ability to operate on an ongoing basis and limit losses in the event of severe business disruption. Such plans must be commensurate with its operational risk profile and Board approved risk appetite towards business disruptions.

103. A bank's business continuity planning must cover all critical business operations and address business disruption events or scenarios associated with these operations.

104. A bank's business continuity management should incorporate business impact analysis, recovery strategies, testing, training and awareness programmes, and communication and crisis management programmes.

105. As with other parts of a bank's operational risk management framework, a bank must periodically review its business continuity plans to ensure contingency strategies remain consistent with current operations, risks and threats, resiliency requirements, and recovery priorities.

106. A bank must ensure business continuity plans are tested periodically to ensure that recovery and resumption objectives and timeframes can be met. Results of formal testing activity should be reported to Senior Management and the Board. Copies of reports must be provided to the CBSI, on request.

(vi) Outsourcing

107. While outsourcing can help a bank manage costs, provide expertise, expand product offerings, and improve services, it also introduces risks that a bank must address.

108. The Board and Senior Management of a bank are responsible for understanding the operational risks associated with outsourcing arrangements and ensuring that effective operational risk management policies and practices are in place to manage the risk in outsourcing activities.

109. A bank's operational risk management framework must encompass, at a minimum:

(a) procedures for determining whether and how activities can be outsourced;

(b) identification, listing and classification of the operating risks generated through outsourcing;

(c) processes for conducting due diligence in the selection of potential service providers;

(d) sound structuring of the outsourcing arrangement, including ownership and confidentiality of data, as well as termination rights;

(e) programs for managing and monitoring the risks associated with an outsourcing arrangement, including the financial condition of the service provider;

(f) establishment of an effective control environment at the bank and the service provider;

(g) development of viable contingency plans;

(h) execution of comprehensive contracts and/or service level agreements with a clear allocation of responsibilities between an outsourcing provider and the bank;

(i) the collection, monitoring, and reporting of data on the bank's outsourcing arrangements, including performance outcomes and risk and any losses generated through outsourcing; and

(j) regular, independent review of outsourcing arrangements in which the bank is engaged.

110. A bank must provide the CBSI with information on outsourcing arrangements to which it is engaged, including copies of contracts or other documentation governing outsourcing, if requested.

111. A bank must promptly notify the CBSI of any adverse, or potential adverse, impact on its operations and its operational risks, arising from problems in its outsourcing arrangements.

(vii) Related parties

112. In the first instance, operational risk generated from a bank's dealings with related parties should be addressed in an equivalent fashion to operational risks arising from dealings with unrelated parties and entities.

113. A bank must collect and record information separately on its operational risk exposures to related parties. This is in addition to the collection and reporting of such exposures as part of the bank's overall operational risk exposures.

114. To the extent that any aspect of a bank's operational risk management framework applicable to non-related parties is not applied to related parties, this outcome must be recorded in a register. This register should also record the source of approval for such outcomes along with details of the reasons, and the level of operational risk exposures arising. Such outcomes should be subject to regular independent review.

115. A bank's operational risk management framework must require staff of the bank to report directly to Senior Management and the Board on any potential conflicts of interest or other operational risk issues of concern that arise from dealings with related parties. The Board and Senior Management are to recognize such advice and to record their response to the issues raised.

116. A bank must provide to the CBSI, if requested, with information (including the register mentioned in Paragraph 110 of this Prudential Standard) on operational risk exposures to related parties, and, more generally, on the application of the bank's operational risk framework to related parties.

(viii) Data Collection

117. The collection of internal loss data is considered to be an essential element to the development and functioning of a credible operational risk measurement system. A bank must collect and maintain internally generated loss data for at least 10 years according to criteria and definitions set out below in Paragraphs 115 to 131 of this Prudential Standard.

118. A bank must have documented policies and procedures for assessing the ongoing relevance of its historical internal loss data. A bank must categorize the operational loss data which collects into various loss event types as indicated in the Annex (Column 1).

119. Internal loss data are most relevant when clearly linked to a bank's current business activities, technological processes and operational risk management procedures. Therefore, a bank must have documented procedures and processes for the identification, approval and collection of internal loss data. Such procedures and processes must be consistent, timely and comprehensive across the bank and subject to validation and regular independent reviews.

120. Assessments of the appropriateness and relevance of data to be collected are to be undertaken on a regular basis and must form the basis of any justification for the exclusion of data from the operational risk data collection. These assessments must be transparent and clearly documented and also subject to regular independent review.

121. A bank's internal loss data must be comprehensive and capture all material activities and exposures. A minimum threshold should be set by the bank, and agreed with the CBSI, for including a loss event in the data collection and calculation of average annual losses. This amount should be subject to review and may change over time.

122. A bank's proposed thresholds for the collection of internal loss data must be appropriate. In determining a threshold, the bank must take into account:

(a) the use of internal loss data for operational risk management; and

(b) the administrative requirements placed on the business lines and operational risk resources as a consequence of the data collection and management processes.

123. A bank must, however, be able to justify that any excluded activities or losses, both individually and in aggregate, would not have a material impact on the overall estimate of the bank's internal loss data.

124. Aside from information on gross loss amounts, the bank must collect information on the following –

(a) the date when the event happened or first began **("date of occurrence")**;

(b) where available; the date on which the bank became aware of the event **("date of discovery")**;

(c) the date (or dates) when a loss event results in a loss, reserve or provision against a loss being recognised in the bank's Profit and Loss accounts **("date of accounting")**; and

(d) descriptive information about the drivers or causes of the loss event. The level of detail of descriptive information must be commensurate with the size of the gross loss amount

125. A bank must develop specific criteria for allocating data arising from an operational risk loss event where business is undertaken in a centralised function, or an activity spans more than one business line.

126. The bank must collect information on recoveries of gross loss amounts.

127. For of the data collection required in this Prudential Standard –

(a) operational loss events related to credit risk should not be included in the loss data set. Operational risk losses that are related to providing credit are losses that arise from the purported exercise of a credit delegation. However, losses arising as a result of fraud perpetuated by parties other than a borrower may be treated as an operational risk loss.

(b) operational risk losses related to market risk should be included in the operational loss data set. Operational risk events that are related to market risk must be reflected in a bank's operational risk profile at the time of discovery (even if positions remain open) and any associated losses recorded in the operational risk loss data collection. Note, however, for the calculation of its market related capital requirement market related transactions must also still be included in any market related risk calculations.

128. A bank must have processes to independently review the comprehensiveness and accuracy of loss data.

129. For the purposes of the data collection required by this Prudential Standard-

(a) **"Gross loss"** is defined as a loss before recoveries of any type;

(b) **"Net loss"** is defined as the loss after taking into account the impact of recoveries.

(c) **"Recovery"** is defined as an independent occurrence, related to the original loss event, separate in time, in which funds or inflows of economic benefits are received from a third party to recoup some or a portion of the original operational loss event - e.g.,

payments received from insurers, repayments received from perpetrators of fraud, and recoveries of misdirected transfers.

130. A bank must be able to identify the gross loss amounts, non-insurance recoveries, and insurance recoveries for all operational loss events. The bank must use losses net of recoveries (including insurance recoveries) in the loss dataset. However, recoveries can be used to reduce losses only after the bank receives payment. Receivables do not count as recoveries. Verification of payments received to net losses must be provided to the CBSI, upon request.

131. The following items must be included in the gross loss computation of the loss data set:

(a) direct charges, including impairments and settlements, to the bank's Profit and Loss accounts and write-downs due to the operational risk event;

(b) costs incurred as a consequence of the event including external expenses with a direct link to the operational risk loss event (e.g., legal expenses directly related to the event and fees paid to advisors, attorneys or suppliers) and costs of repair or replacement, incurred to restore the position that was prevailing before the operational risk event;

(c) provisions or reserves accounted for in the bank's Profit and Loss accounts against the potential operational loss impact;

(d) losses stemming from operational risk events with a definitive financial impact, which are temporarily booked in transitory and/or suspense accounts and are not yet reflected in the Profit and Loss accounts ("pending losses");

(e) material pending operational risk losses should be included in the loss data set within a time period commensurate with the size and age of the pending item; and

(f) negative economic impacts booked in a financial accounting period, due to operational risk events impacting the cash flows or financial statements of previous financial accounting periods (timing losses"). Timing impacts typically relate to the occurrence of operational risk events that result in the temporary distortion of a bank's financial accounts (e.g., revenue overstatement, accounting errors and mark-to-market errors). While these events do not represent a true financial impact on the bank (net impact over time is zero), if the error continues across more than one financial accounting period, it may represent a material misrepresentation of the bank's financial statements; and

(g) material "timing losses" should be included in the operational risk loss data set when they are due to operational risk events that span more than one financial accounting period and give rise to legal risk.

132. For the purposes of the required data collection, the following items should be excluded from the gross loss computation of the loss data set:

(a) costs of general maintenance contracts on property, plant or equipment;

(b) internal or external expenditures to enhance the business after the operational risk losses: upgrades, improvements, risk assessment initiatives and enhancements; and

(c) insurance premiums.

133. A bank must use the date of accounting for building the operational risk loss data set required to be collected in accordance with this Prudential Standard. The bank must use a date no later than the date of accounting for including losses related to legal events in the loss data set. For legal loss events, the date of accounting is the date when a legal reserve is established for the probable estimated loss in the bank's Profit and Loss accounts.

134. Losses caused by a common operational risk loss event or by related operational risk loss events over time, but posted to the accounts over several years, should be allocated to the corresponding years of the loss database, in line with their accounting treatment.

ANNEX

Detailed Classification of Operational Risk Loss Events

Event-Type Category	Definition	Sub-Categories	Activity Examples (Level 3)
1	2	3	4
Internal Fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/discrimination events, which involves at least one internal party	Unauthorized Activity	Transactions not reported (intentional) Transaction type unauthorized (w/monetary loss) Mismarking of position (intentional)
		Theft and Fraud	Fraud / credit fraud / worthless deposits Theft / extortion / embezzlement / robbery Misappropriation of assets Malicious destruction of assets Forgery Check kiting Smuggling Account take-over / impersonation / etc. Tax non-compliance / evasion (wilful) Bribes / kickbacks Insider trading (not on firm's account)
External Fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party	Theft and Fraud	Theft/Robbery Forgery Check kiting
		Systems Security	Hacking damage Theft of information (w/monetary loss)
Employment Practices and Workplace Safety	Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal injury claims, or from diversity / discrimination events	Employee Relations	Compensation, benefit, termination issues Organized labour activity
		Safe Environment	General liability (slip and fall, etc.) Employee health & safety rules events Workers compensation
		Diversity and Discrimination	All discrimination types
Clients, Products and Business Practices	Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients (including	Suitability, Disclosure, and Fiduciary	Fiduciary breaches / guideline violations Suitability / disclosure issues (KYC, etc.) Retail customer disclosure violations Breach of privacy Aggressive sales Account churning

	fiduciary and suitability requirements), or from the nature or design of a product.		Misuse of confidential information Lender liability
		Improper Business or Market Practices	Antitrust Improper trade / market practices Market manipulation Insider trading (on firm's account) Unlicensed activity Money laundering
		Product Flaws	Product defects (unauthorized, etc.) Model errors
		Selection, Sponsorship, and Exposure	Failure to investigate client per guidelines Exceeding client exposure limits
		Advisory Activity	Disputes over performance of advisory activities
Damage to Physical Assets	Losses arising from loss or damage to physical assets from natural disaster or other events.	Disasters and Other Events	Natural disaster losses Human losses from external sources (terrorism, vandalism)
Business Disruption and System Failures	Losses arising from disruption of business or system failures	Systems	Hardware Software Telecommunications Utility outage / disruptions
Execution, Delivery, and Process Management	Losses from failed transaction processing or process management, from relations with trade counterparties and vendors	Transaction Capture, Execution, and Maintenance	Miscommunication Data entry, maintenance or loading error Missed deadline or responsibility Model / system mis-operation Accounting error / entity attribution error Other task mis-performance Delivery failure Collateral management failure Reference Data Maintenance
		Monitoring and Reporting	Failed mandatory reporting obligation Inaccurate external report (loss incurred)
		Customer Intake and Documentation	Client permissions / disclaimers missing Legal documents missing / incomplete
		Customer/Client Account Management	Unapproved access given to accounts Incorrect client records (loss incurred) Negligent loss or damage of client assets
		Trade Counterparties	Non-client counterparty mis performance Misc. non-client counterparty disputes
		Vendors and Suppliers	Outsourcing Vendor disputes