AIIB Directive on
Operational Risk Management
March 7, 2019

1. Overriding Objective

1.1. This Directive sets out the high-level principles of the Bank's Operational Risk Management Framework. It establishes a consistent definition of Operational Risk, and sets out the core principles, processes and methodologies through which the management of Operational Risk is achieved. Further, it establishes the governance and accountabilities which support Operational Risk Management (ORM) within the Bank.

1.2. The exercise and interpretation of this Directive shall be consistent with the AIIB Risk Management Framework and seeks to give effect to this overriding objective and to ensure that the Bank's Operational Risks are managed to within acceptable levels in view of the Bank's Risk Appetite.

2. General Principles

2.1. The Asian Infrastructure Investment Bank, through the execution of its typical business functions, is exposed to Operational Risk.

2.2. It is not possible to avoid Operational Risks and the potential for associated financial and non-financial losses. However, it is possible to mitigate such losses through sound governance and appropriate policies and procedures.

2.3. The purpose of Operational Risk management within the AIIB is to reduce the likelihood and consequences of avoidable Operational Risk events. The key benefits of effective Operational Risk Management include improved performance, reduced costs, increased accountability and protection against reputational damage.

2.4. Given that Operational Risk is associated with every activity in the Bank, Operational Risk Management needs to be embraced by all Bank personnel.

2.5. Operational Risk events may trigger the need for a business continuity response. The Bank has a comprehensive approach to Business Continuity Management (BCM) which addresses its response to a broad range of potential major operational disruptions involving material unavailability of staff, premises, systems, or key suppliers, or a combination of both.

3. Definitions

3.1. **Business Unit**
A Vice-Presidency, Department or Division of the Bank, or discrete subcomponent thereof.

3.2. **Operational Risk**

3.2.1. The Bank's defines Operational Risk as the risk of loss, or detriment, resulting from inadequate or failed processes or systems, through human error, or from the occurrence of external events.

3.2.2. The Bank's definition of Operational Risk is consistent with the Basel Committee Banking Industry Standards but has been extended to include Reputational Risk[1].

3.2.3. Losses arising from strategic risk[2] are not considered Operational Risk events.

3.3. **Reputational Risk**

3.3.1. This refers to the risk arising from any of the Bank's activities that could adversely impact its reputation, standing or public esteem. Adverse reputation directly impacts how the Bank is regarded by customers, suppliers, existing and potential employees, investors, interest groups, rating agencies and shareholders.

3.3.2. Reputational risk is a consequential risk, generally triggered by an Operational Risk failure. Reputational risk is, however, extremely difficult to assess.

3.3.3. It is the responsibility of all Bank personnel to guard the reputation of the Bank.

4. Governance and Responsibilities

Good corporate governance is assured by the open communication and oversight of Operational Risk issues. Operational Risk management requires the attention and involvement of a wide variety of organizational components, each with clear roles and responsibilities to fulfill. Line managers have primary responsibility for managing Operational Risk within their respective business areas.

4.1. **Risk Committee (RC)**

Matters arising under this Directive that cannot be resolved between respective functions shall be brought to the Risk Committee.

1 Operational Risk should not be confused with Project Risks. Project Risks are governed by the Bank's Operational Policies, including the Policy on Financing, Environmental and Social Policy, Procurement Policy, Policy on International Relations, and Policy on Prohibited Practices.

2 Strategic risk is the current and prospective risk to earnings or capital arising from the untimely, lack of, or improper implementation of decisions, or lack of responsiveness to industry changes. The risk is a function of the capability of an organization's strategic goals, the business strategies developed to achieve those goals, the resources deployed against those goals and the quality of implementation. Strategic risk includes the risk that the Bank's strategy may be inappropriate to support sustainable future growth.

4.2. **Risk Management Department**

The Risk Management Department, independent of the Business Units, shall take the lead in the ongoing implementation of the Operational Risk Framework. This is closely coordinated within an overall risk management framework. Overall planning, coordination and monitoring shall be provided by a centralized Operational Risk Management (ORM) function within the Risk Management Department (RMD).

4.3. **Business Unit Management (Operational Risk Owners)**

Business Units have primary responsibility for managing Operational Risk within their respective business areas and in those products, activities, processes and systems for which they are responsible in close cooperation with the Operational Risk Management function, the Compliance function, and other specialist units and departments referenced below. In this respect they are responsible for ensuring that the management of Operational Risk is embedded in the day-to-day activities of the unit.

The heads of Business Units shall ensure that:

a. Risk issues and/or any breakdown in controls in their Business Unit are proactively managed, monitored, and corrective action taken immediately to address these matters.
b. Operational Risk incidents (events) in their Business Unit are reported.
c. The Risk Management Department is informed of proposals regarding new, or significantly changed material products, activities, processes and systems.

4.4. **Bank Personnel**

All Bank Personnel are expected to contribute actively to the management of Operational Risk at the AIIB. Personnel are responsible for:

a. Ensuring that they are familiar with the policies and procedures governing their responsibilities.
b. Identifying key Operational Risk exposures and the breakdown or weakness in internal controls.
c. Disclosing any operational loss, incident, failure or error of which they are aware to the appropriate line manager.

4.5. **Specialist Business Units**

The specialist Business Units listed below shall cooperate closely with the Risk Management Department and one another to assist in identifying, assessing, monitoring, mitigating and controlling specific Operational Risks.

a. Office of the General Counsel (OGC)
b. Human Resources Department (HRD)
c. Information Technology (ITD)
d. Facilities and Services (FAS)
e. Office of the Controller (CTL)

5. Operational Risk Management Framework

5.1. Each aspect of the typical risk management processes has been recognized and incorporated into the Bank's Operational Risk Management Framework which provides a continuous and reiterative process of risk identification, validation, management and review.

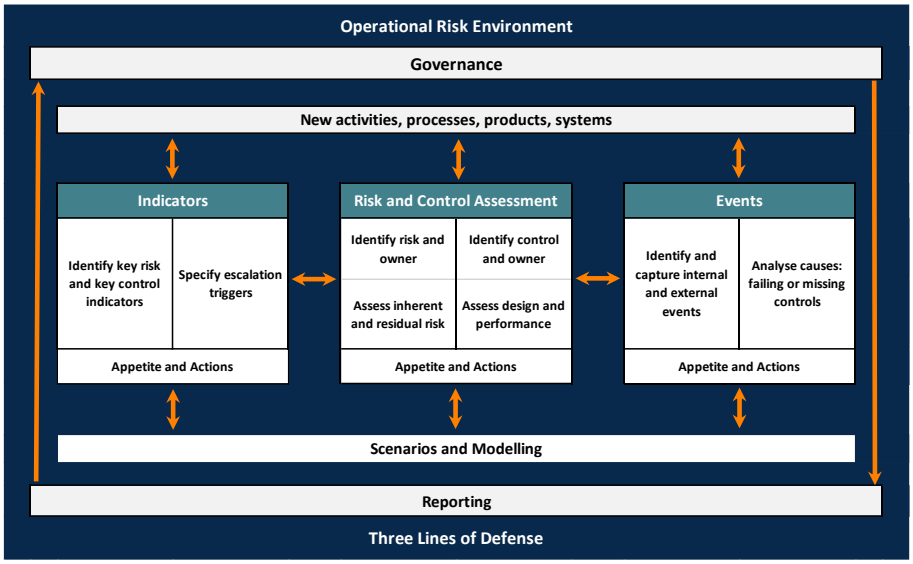

Figure 1: AIIB Operational Risk Management Framework

6. Risk Identification and Assessment

This section describes the key elements of the Operational Risk Framework, including tools and methods used to identify and assess Operational Risk within AIIB.

6.1. Operational Risk and Control Self-Assessment (RCSA)

Risk owners shall be responsible for the identification, assessment and treatment of Operational Risks to reduce the residual exposure to within acceptable levels, document the Operational Risk profile and control measures in a risk register, and conduct self-assessments of the effectiveness of risk controls. These are facilitated by the Risk Management Department.

6.2. Specialist Assessments

Business Units may seek advice from specialist services and units in identifying and assessing specific Operational Risks, with which the business areas concerned may not be familiar. The risks identified by these services supplement the risk identification and assessment process.

6.3. Key Risk Indicators (KRI)[3]

Risk owners shall be responsible for identifying Key Risk Indicators, including limits and thresholds, for all significant Operational Risks. These Key Risk Indicators shall be rigorously measured, monitored and reported on both at departmental and entity levels.

3 Key Risk Indicators are metrics that provide insight into Operational Risk exposure, the potential for losses, and the effectiveness of existing controls.

6.4. **Operational Risk Incident Reporting**
Business Unit management shall ensure that all Operational Risk incidents (also termed Operational Risk events) and significant Operational Risk exposures are reported to Risk Management Department.

6.5. **External Loss Data**[4]
The Risk Management Department shall, as appropriate, use external loss data to identify potential Operational Risk exposures, to inform Operational Risk quantification and, if relevant, for scenario analysis.

6.6. **Scenario Analysis**[5]
The Bank shall use scenario analysis to identify and assess low-frequency, high-severity Operational Risk exposures, in instances where there is insufficient relevant internal or external loss data.

6.7. **Audit Reports**
Reports produced by the Internal Audit Office and the Bank's external auditors may also serve to identify Operational Risk exposures and control weaknesses.

6.8. **New and significantly amended products, activities, processes and systems**
The Chief Risk Officer shall define, establish and oversee a process to be followed by the Bank regarding the introduction of new and significantly amended products, activities, processes and systems.

7. Risk Measurement and Analysis

7.1. Operational risk assessments are conducted within a consistent methodology determined by the Risk Management Department at various levels to measure, analyze and evaluate Operational Risk implications which inform the Bank's planning, decision-making and change management processes.

7.2. The Risk Management Department shall model the behavior of Operational Risk losses by estimating their frequency and severity to produce an estimate of the potential Operational Risk losses that could be suffered by the Bank, at an appropriate confidence interval over a one-year period. The confidence interval is determined by the Chief Risk Officer.

8. Risk Monitoring and Reporting

8.1. Risk owners are responsible for identifying and monitoring Key Risk Indicators for all significant Operational Risks.

8.2. The Risk Management Department shall monitor the overall Operational Risk exposure of the Bank is within Risk Appetite.

4 External Loss Data refers to operational losses suffered by other institutions. The data is filtered so that only external loss data relevant to the Bank is considered.
5 Scenarios describe a sequence of hypothetical events that could have a severe impact on the organization if they occur.

8.3. The Risk Management Department shall consolidate information in regular reports to the appropriate level of Management.

9. Risk Controlling and Mitigation

Operational Risk shall be controlled and/or mitigated using a variety best practice and organizational structures.

10. Training, Communication and Awareness

The Risk Management Department is responsible for coordinating the training of Bank personnel to enable them to own and manage Operational Risk. It is then their responsibility to cascade this knowledge and promote Operational Risk ownership across their teams.

11. Information Disclosure by AIIB

The Bank's Public Information Policy and its related Directive and Administrative Guidance governs the disclosure of all information in the Bank's possession, including with respect to this Directive. Any such disclosure should be consistent with any duty of confidentiality owed to the Bank, its customers, staff and other stakeholders.

12. Authority

The Chief Risk Officer shall make all final decisions regarding the application of this Directive.

13. Implementation

The Chief Risk Officer shall oversee this Directive and introduce any related Administrative Guidance and ensure their efficient and accurate implementation.

This Directive revokes and replaces the Directive on Operational Risk Management of December 11, 2018.