AIIB Directive on
The Risk Appetite Framework
[Effective Date, October 25, 2018]

1. Overriding objectives

1.1 This directive (Directive) on the Risk Appetite Framework (RAF) establishes the rules and processes to formulate, monitor and review the Bank's Risk Appetite Statement (RAS)[1].

1.2 The exercise and interpretation of this Directive shall seek to give effect to this overriding objective.

2. Overview and General Principles

2.1 The RAF considers all material risks of the Bank and sets out controls and processes to monitor and report such risks. The RAF complements the Risk Management Framework and provides a detailed articulation of the responsibilities of the Risk Management Department (RMD) as they pertain to the Bank's Risk Appetite.

2.2 The RAF is based on the following key principles:

- It must align the Bank's Risk Capacity with its long-term vision and strategic objectives.
- It must be dynamic and reflect changes in the Bank's business profile.
- It must articulate clear requirements, roles and responsibilities.
- It must be comprehensive, cover all forms of material risk and establish metrics to measure risks.
- It must be employed ex-ante when assessing the risk contribution of the marginal lending/investment opportunity

[1] AIIB's inaugural Risk Appetite Statement was established in December 2017 (Sec2017-146)

3. Definitions

3.1 **Risk Appetite.** The maximum aggregate level and types of risk the Bank is willing to assume, within its Risk Capacity, to achieve its strategic objectives and business plan.

3.2 **Risk Appetite Statement** (RAS). The Bank's statement that:

a. acknowledges the specific risk parameters of AIIB's business model,
b. articulates the level of risk the Bank is willing to take (or not take) along those dimensions,
c. puts in place systems to identify, monitor and minimize those risks, and
d. aligns business planning, budget and incentives, to the Bank's Risk Appetite and enables the Bank to achieve its mission.

3.3 **Risk Capacity.** The maximum level of risk the Bank can assume given its current level of resources before breaching constraints determined by: its available capital and liquidity needs; the operational environment (e.g. technical infrastructure, risk management capabilities, expertise) and obligations.

3.4 **Risk Profile.** The point-in-time assessment of the Bank's gross and, as appropriate, net risk exposures (after considering risk mitigation factors) aggregated within and across each relevant risk category based on forward-looking assumptions. These assumptions include those on how the risk profile may change under both expected and stressed economic conditions.

3.5 **Key Risk Indicators (KRIs)**. Metrics used to assess risk.

3.6 **Key Performance Indicators (KPIs)**. Metrics used to assess performance.

4. Risk Appetite

4.1 The Chief Risk Officer (CRO) shall present to the Risk Committee (RC) the Bank's RAS based on the Bank's overall Risk Profile, future risk strategy and Risk Capacity.

4.2 Each year the Board will be asked to approve the specific levels of top-down allocation and renew their support for the RAS.

4.3 To ensure comprehensiveness, all risk types must be considered within the establishment of the RAS. RMD shall ensure that the Bank's assessment of risks reflects industry best practice and Basel guidance as appropriate.

4.4 The Bank shall allocate its Risk Capacity between core and non-core risks in the following manner:

Core risks: Directly linked to the Bank's mandate through its investment operations

Non-Core risks: Factors which arise from activities supporting the Bank's mandate, including treasury operations and operational risk

4.5 Each risk type shall be classified as being either: low, medium or high appetite, which shall indicate the impact of the event, as well its probability of occurrence.

4.6 KRI / KPIs shall be classified into one of three levels based on materiality (as highlighted in the table below). Modifications to such classifications shall require the corresponding agreement from the owner.

KRI Level	Owner	Monitoring Department	Monitoring Process	Minimum Reporting Frequency
1	Board	RMD	RC → ExCom → Board	Annually
2	President	RMD	RC → ExCom	Quarterly
3	Vice President (VP) / Departmental	Corresponding Department	VP	Monthly

4.7 For financial risks, a limits framework shall be implemented to monitor related KRIs for each risk type. Risk limits shall be incorporated into the Bank's strategy plan and updated at least annually. These shall be measured using upper and lower limits to monitor where the Risk Profile sits against appetite.

4.8 For non-financial risks, KRIs for each risk type will be monitored against the lower limit only.

4.9 For both cases in the event of a limit being inappropriate due to the inability of the Bank to mitigate the outcome, the metric shall be regarded as a KPI and measured using targets rather than limits.

4.10 The President's Level 2 KRI / KPIs will be established through the issuance of a standalone directive.

5. Monitoring and Review

5.1 KRIs / KPIs shall be assessed at least annually to ensure they remain fit for purpose.

5.2 Each KRI / KPI shall have a designated data provider corresponding to the business line, who shall provide the monitoring department the necessary position level information.

5.3 RMD shall stress the Bank's draft business plan as developed by Policy and Strategy to ensure its compliance with the RAS using the determined severe and protracted scenario.

5.4 RC shall inform the Board of the impact of the Business Plan upon the RAS, with explanations as to any remedial actions in the event the Business Plan causes the RAS to be breached.

5.5 RMD shall monitor Level 1 and 2 KRIs monthly to determine their status, reporting in accordance with table above to their owners[2]. A limit breach is defined as when the actual or stressed KRI exceeds its limit (or target, as appropriate). Breaches shall be escalated to the KRI owner by the route outlined in the table above, together with a clear justification of such breach as well as a management plan to correct the breach / deviation.

5.6 VPs shall inform the CRO of their Level 3 KRIs.

6. Information Disclosure by AIIB

6.1 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.

7. Implementation

7.1 The CRO shall oversee this Directive and introduce any related Administrative Guidance and ensure their efficient and accurate implementation.

8. Authority

The CRO shall make all final decisions regarding the application of this Directive.

[2] ExCom shall also be informed of the KRI Level 1s on a quarterly basis.