Operational Risk Exposure Disclosure

31 December 2020

I. Operational Risk Calculation

Quantitative Operational Risk Disclosure – Bank Stand Alone

(in million Rupiah)

No	Approach	31 December 2020			31 December 2019		
		Gross Income (average 3 years)	Capital Charge	RWA	Gross Income (average 3 years)	Capital Charge	RWA
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
1	Basic Indicator Approach	8.451.193	1.267.679	15.845.987	7.293.907	1.094.086	13.676.076
	Total	8.451.193	1.267.679	15.845.987	7.293.907	1.094.086	13.676.076

Quantitative Operational Risk Disclosure – Consolidated Bank and Subsidiary

(in million Rupiah)

No	Approach	31 December 2020			31 December 2019		
		Gross Income (average 3 years)	Capital Charge	RWA	Gross Income (average 3 years)	Capital Charge	RWA
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
1	Basic Indicator Approach	12.441.111	1.866.167	23.327.084	9.819.730	1.472.960	18.411.994
	Total	12.441.111	1.866.167	23.327.084	9.819.730	1.472.960	18.411.994

II. General Qualitative Disclosure

Operational risk is defined as the risks of loss resulting from inadequate or failed internal processes, people, systems failure or external events that impacted to the bank's operational activities.

1. Operational Risk Management Governance

The Board of Commissioners and the Board of Directors actively supervise operational risk management through various committees such as the Risk Monitoring Committee and the Risk Management Committee which carried out periodically according to their respective terms of reference to discuss operational risks and its implementation, authority and responsibilities.

ORM (Operational Risk Management) unit, which has direct reporting line to the Risk Management Director, is responsible for operational risk management. The Bank has formulated and determined the level of operational risk sufficiently in line with the objectives and business strategy of the Bank. The level of operational risk is translated into the operational risk appetite and documented in the Operational Risk Management Framework.

2. Adequacy of Policies, Procedures, and Determination of Limits

Operational Risk Management unit is responsible in establishing and developing Operational Risk Management policies and procedures. These policies and procedures are reviewed periodically, taking into account any significant changes, both internally and externally. Each working unit must comply with operational risk management policies and procedures in carrying out its day-to-day operational activities. The Bank also has a system and limits to support general and specific controls, such as segregation of duties and responsibilities, mandatory annual leave, reconciliation and others.

3. Adequacy of the Identification, Measurement, Monitoring and Risk Control Processes as well as Risk Management Information System

Operational risk identification is carried out for all activities / processes, products, systems and organizations. A part from being carried out on the Bank's new initiatives, risk assessments are also carried out on developments or changes. The operational risk identification process is also equipped with operational risk management tools including Risk Grading Matrix, Risk Registration, KORI (Key Operational Risk Indicator) and Risk Acceptance.

The risk measurement process includes periodic self-assessment through KCSA (Key Control Self Assessment), analysis of operational events and losses, implementation of inspection activities by ICR, measurement of Key Operational Risk Indicators (KORI), preparation of operational risk appetite which are reported periodically in Risk Management Committee (RMC) meeting.

Operational risk monitoring is carried out through reporting to senior management and regulators, either regularly or ad-hoc, including reporting of significant incidents through SINP (Significant Incident Notification Protocol). Implementation of SINP will ensure that any significant problems can be immediately followed up.

Operational risk control is also carried out by implementing effective prevention, detection and correction control mechanisms and / or providing adequate insurance to minimize the impact of operational losses for the Bank. As one of the control measures, Bank already has comprehensive guidelines for Business Continuity Management which refers to the industry standard ISO-22301 and tested regularly.

Operational Risk Management System (ORMS) is available to provide accurate, timely and up-to-date information to facilitate analysis and decision making.

4. Internal Control System for Operational Risk

Internal control over operational risk is carried out through three lines of defense model. In the first line of defense, the Risk Taking Unit (RTU) assisted by Business Risk / ICR carries out day-to-day operational risk

management. In the second line of defense, the ORM unit is tasked with identifying and measuring inherent risks and ensuring the adequacy of the control mechanisms that have been implemented.

In the third line of defense, Internal Audit is independently responsible for ensuring that the residual risks are still within the limits that can be tolerated by the Bank. Alignment process between the parties responsible for the Bank's internal control practices is carried out on a sustainable basis through a standardize ICR Maturity Self-Assessment and forums which organized by ORM unit to facilitate ICR function.

5. Fraud Risk Management

The Bank has adequate policies and procedures of anti-fraud strategies which continue to be refined. Fraud risk management is systematically managed through a number of processes/strategies.

Regarding the process of fraud risk prevention, the Bank has implemented risk awareness, anti-fraud awareness and the requirement of integrity pact that must be signed by the Board of Directors, Board of Commissioners, and all employee. Regular update on the policies and procedures related to anti-fraud strategies to ensure its relevancy with the latest conditions and perform risk assessment on each initiative proposal, product and Bank activities, both new and in development. Anti-fraud awareness socialization is performed through several medias, namely e-newsletter and email broadcasts, PC/ laptop desktop wallpapers, standing acrylics, comic strips on B-Connect, BTPN Info, anti-fraud animated video broadcasts, additional information on whistleblowing services on Bank BTPN website that can be used to reporting fraud incidents, mandatory anti-fraud assessments through e-learning, anti-fraud declarations through e-learning and anti-fraud awareness delivered in in-class training and online training to employees.

In line with the prevailing anti-fraud strategy, Bank continuously disseminate reports on fraud indication events through whistleblowing channel as one of media used for detecting fraud incidents, which periodically communicated to all employees through the Bank's various internal media. Through whistleblowing channel as one of media used for detecting fraud incidents: e-mail channel (Speak Your Mind, Ayo Lapor), Whatsapps, Phone, Letter and face to face meeting, an employee may reveal and report any misconduct occurred in the Bank.

Bank also has adequate policies related to fraud investigation and reporting processes. For any proven fraud case, sanction will be imposed and decided by Fraud Committee which also involves relevant work units, relevant Business Risk/ICR Functions, Human Capital unit and Anti-Fraud Management (AFM) unit. Fraud Committee's decision is regularly monitored and evaluated for future improvements.