Risk Exposure Publication Report – Operational

31 December 2021

I. Operational Risk Calculation

Quantitative Operational Risk Disclosure – Bank Stand Alone

(in million Rupiah)

No	Approach	31 December 2021			31 December 2020		
		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	8.688.851	1.303.328	16.291.596	8.451.193	1.267.679	15.845.987
	Total	8.688.851	1.303.328	16.291.596	8.451.193	1.267.679	15.845.987

Quantitative Operational Risk Disclosure – Consolidated Bank and Subsidiary

(in million Rupiah)

No	Approach	31 December 2021			31 December 2020		
		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	12.343.405	1.851.511	23.143.885	12.441.111	1.866.167	23.327.084
	Total	12.343.405	1.851.511	23.143.885	12.441.111	1.866.167	23.327.084

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 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 that conducted periodically in accordance with terms of reference to discuss operational risks and its implementation.

Operational Risk & Anti Fraud Management (OR&AFM) Division, which has a direct reporting line to the Risk Management Director, is responsible for operational and fraud risk management. The Bank had formulated and determined the profile and level of operational risk sufficiently to be in line with overall business goals and strategies of the Bank. Monitoring the operational risk profile and level is carried out through operational risk management tools, such as operational risk appetite and key risk indicators which are part of the operational risk management framework.

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

OR&AFM Division is responsible for the formulation and development of Operational Risk Management policy and procedure and reviewed periodically to considers for any significant changes, both internal and external.

Each work unit must adhere to operational risk management policies and procedures in carrying out daily operational activities. Bank also has system and determination of limits to support common and specific controls, such as segregation of duties, annual mandatory block leave reconciliation and others.

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

The process of operational risk management including identification, measurement, monitoring and risk control runs in a structured and consistent manner. The Operational Risk Management process in Bank implemented based on effective best practices which also includes Business Continuity Management and Information Security Management.

The operational risk management process which includes identification, measurement, monitoring and control of operational risk are describe as follows:

1. Operational risk identification is carried out on process, product, system, initiative and organization for new and changes. The operational risk identification is also performed through operational risk management tools such as Risk Grading Matrix (RGM), Process Risk Control (PRC), Key Risk Indicator (KRI) and Risk Acceptance (RA).
2. Risk measurement process includes periodic self-assessment activities through Key Control Self Assessment (KCSA), analysis of operational risk events and losses, inspection activities by Internal Control & Risk (ICR), KRI measurement and Operational Risk Appetite (ORA) which is reported monthly in meetings of Risk Management Committee (RMC).
3. Operational risk monitoring is carried out through reporting to senior management and regulators, either on a regular basis or on an ad-hoc basis, including reporting events with significant incident through SINP (Significant Incident Notification Protocol). This is implemented so that any problems that occur can be immediately followed up.
4. Operational risk control is also carried out by implementing effective prevention, detection and correction control mechanisms and/or providing adequate insurance to minimize the impacts of operational losses on Bank. As one of the control measures, Bank has guidelines for comprehensive Business Continuity Management which refer to the ISO-22301 industry standard which is tested regularly

The Internal Control & Risk System (ICRS – previously Operational Risk Management system/ORMS) is provided to provide accurate, timely and up-to-date information needs to facilitate analysis and decision making.

The calculation of the Capital Adequacy Assessment Process (ICAAP) for operational risk is currently carried out by Bank and Subsidiary using the Basic Indicator Approach. Furthermore, ICAAP computation with the Standardized Approach will be carried out according to the schedule set by the Financial Services Authority.

The Bank and its Subsidiaries already have guidelines for comprehensive business continuity management and refer to the ISO 22301 industry standard, with the aim of anticipating operational risks that may occur from extreme/critical situations due to natural disasters such as floods, earthquakes and other factors such as fires, disturbances on power supply systems, to unfavorable business situations. This is to ensure continuity of service to customers is guaranteed.

Since the beginning of COVID-19 virus outbreak in Indonesia, Bank continuously makes effort to minimize the impact of COVID-19 virus outbreak at the office environment by establishing a Task Force which is directly led by the President Director. The Task Force's main purpose is to establish and implement anticipative approaches which are aligned with the government program to ensure that Bank can still operate its operational activities with minimum disruption.

4. Internal Control System for Operational Risk

Internal control system for operational risk is carried out through the implementation of three lines of defense models. In the first line of defense, the Risk Taking Unit (RTU) assisted by Business Risk/ICR carried out dayto-day operational risk management. In the second line of defense, the OR&AFM work unit is overseeing the implementation of risk management process to ensure the implementation in accordance with stipulated procedure.

In the third line of defense, Internal Audit is independently responsible for ensuring that residual risks are still within the limits that can be tolerated by Bank.

Alignment process between the parties responsible for Bank's internal control practices is carried out on an ongoing basis through a standardized ICR (ICR maturity self-assessment) matrix and forums organized by the OR&AFM work unit to facilitate the Internal Control & Risk function.

5. Fraud Risk Management

BTPN has no tolerance to any fraud incident. Bank always follows up on every fraud incident including providing sanctions to employees who commit or are involved in fraud incidents as per prevailing regulations including reporting to the authorities (if necessary).

Bank has adequate policies and procedures of antifraud strategies which are continuously improvised. Fraud risk management is systematically handled through a series of process and strategy.

In relation to fraud risk prevention process, the Bank has implemented anti-fraud awareness program for all employees and the signing of integrity pact by the Board of Directors, Board of Commissioners, and every Bank employee. Adjustments to policies and procedures for managing anti-fraud strategies are carried out regularly to be in line with current conditions. In addition, both new and development products, processes, systems and initiatives are assessed for potential fraud risk.

Anti-fraud socialization and awareness was carried out through several media, namely e-newsletters, email broadcasts, desktop PC/laptop wallpapers, standing acrylics, BTPN Info, anti-fraud animation videos, anti-fraud mandatory e-learning, implementation of anti-fraud declarations and in-class or virtual anti-fraud awareness training to employees. In addition, there is whistleblowing chanel provided by Bank for reporting indication of fraud.

Bank provides anti-fraud awareness training and Entertainment & Gifts to third parties particularly vendors, on a regular basis to participate in assisting the Bank in maintaining good governance.

In line with the applicable anti-fraud strategy, Bank also continuously socialized the reporting through whistleblowing channel for detecting fraud incident, which is regularly communicated to all employees through various internal Bank media. Employees can disclose and report any violations (misconduct) through e-mail channels (Speak Your Mind, Ayo Lapor), Whatsapps, telephone, letters or face-to-face meetings.

The Bank has adequate policies regarding investigation process and reporting of fraud. For each proven fraud case, the process of imposing sanctions is decided by Fraud Committee involving the relevant work units, related Business Risk/ICR Functions, Human Resources and OR&AFM unit. The implementation of Fraud Committee's decisions is monitored and evaluated periodically to determine future improvement efforts.