Risk Exposure Publication Report – Operational

31 December 2023

I. Operational Risk Calculation

Quantitative Operational Risk Disclosure – Bank Individual

(in million Rupiah)

No	Approach	31 December 2023			31 December 2022		
		Business Indicator Component (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				8.624.711	1.293.707	16.171.334
2	Standardized Approach	818.034	818.034	10.225.432			
	Total	818.034	818.034	10.225.432	8.624.711	1.293.707	16.171.334

Quantitative Operational Risk Disclosure – Bank Consolidated with Subsidiary

(in million Rupiah)

No	Approach	31 December 2023			31 December 2022		
		Business Indicator Component (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				12.435.609	1.865.341	23.316.768
2	Standardized Approach	840.067	840.067	10.500.841			
	Total	840.067	840.067	10.500.841	12.435.609	1.865.341	23.316.768

RISK MANAGEMENT IMPLEMENTATION REPORT
FOR OPERATIONAL RISK

Bank Name: BTPN (individual)
Reporting Year: 2023 /(Audited)

1	**Explanation of regulations, policies and/or guidelines related to risk management for Operational Risk.** BTPN (hereinafter referred to as "Bank") has policies and procedures for operational risk management. These policies and procedures are reviewed periodically with consider any changes in Bank's internal and external factors, especially related to regulatory requirement. All work units in Bank must be guided by these policies and procedures in carrying out their daily operational activities. Policies and procedures related for Operational Risk Management are: • Operational Risk Management Policy • Business Continuity Management Policy • Insurance Management Policy • Information Security Management Policy • Key Control Self-Assessment (KCSA) procedure • Key Risk Indicator (KRI) procedure • Event Registration and Booking of Operational Risk (RLED) procedure • Significant Incident Notification Protocol (SINP) procedure • Operational & Fraud Risk Assessment (KROF) procedure • Internal Control and Risk (ICR) implementation procedure • Risk Grading Matrix (RGM) and Process Risk Control (PRC) procedure • Operational Risk Appetite (ORA) procedure • Risk Acceptance (RA) Procedure • Information Management and Security (POS) procedure • Risk Control Meeting (RCM) procedure • Business Impact Analysis (BIA) and Business Continuity Plan (BCP) procedure • Incident Management Plan (IMP) procedure • Initiative Management procedure • 2nd LoD Roles and responsibilities procedure • Anti Fraud Strategy procedure • Investigation procedure • Whistleblowing procedure • Fraud Reporting and Monitoring Procedure
2	**Explanation of the structure and organization of management and control function related to Operational Risk.** Bank using 3 lines of defense model to divide the role and responsibilities of each party within the Bank's organization for the implementation of Operational Risk Management. **In the first line of defense,** all business and support functions work unit as risk owners who are directly responsible for the implementation of operational risk management. In its implementation, the work unit is supported by Business Risk. Besides supported by Business Risk, at the operational level Bank has ICR (Internal Control & Risk) function that responsible to support related work unit in managing their daily operational risk.

	The role and responsibilities of business and support functions work unit are: • Identify and register all operational inherent risks in each product, service, process, and initiative. • Record risk events and book operational risk losses and recovery. • Follow-up action for operational and fraud risk events and its completion. • Carry out all operational risk management program that has determined by OFRM Division. The role and responsibilities of the ICR (Internal Control & Risk) function are: • Act as coordinator in the implementation and completion of operational risk management implementation programs in their respective areas. • Assist work units in providing operational risk review. • Assist work units in issue resolution or operational risk events. • Conduct inspections and report each finding to the relevant parties. • Monitor follow-up action and resolution of each identified finding. **In the second line of defense,** is Operational & Fraud Risk Management (OFRM) Division which has direct reporting line to the Head of Risk Management, responsible for operational and fraud risk management. The roles and responsibilities of the OFRM Division are: • Create and develop operational and fraud risk management policies, procedures and tools. • Create operational and fraud risk management implementation programs. • Provide socialization and training on operational and fraud risk management to work units. • Support work units in providing operational and fraud risk review. • Create operational and fraud risk report to management and regulator. • Monitoring the implementation of operational and fraud risk management in Bank. • Create and develop ICRS (Internal Risk & Control system) as application used to manage operational risk in Bank. **In the third line of defense,** is Internal Audit to conduct inspection and evaluation of governance and implementation of operational risk management. Examination is carried out on the first line of defense and the second line of defense. The Board of Commissioners and Directors supervise the implementation of Operational Risk Management through the Risk Monitoring Committee and Risk Management Committee which are conducted regularly. The roles and responsibilities of the Board of Commissioners are: • Evaluate and approve policies and strategic plans for the implementation of operational and fraud risk management. • Monitor Operational Risk Appetite. • Provide direction on the implementation of operational and fraud risk management. The roles and responsibilities of Directors are: • Ensure the adequacy of the organizational structure and human resource for the implementation of operational risk management in their respective areas. • Ensure the implementation of operational risk management program has been carried out. • Monitor and ensure follow-up resolution of any operational issues or risk event and fraud event. • Develop awareness culture of operational and fraud risk.
3	**Explanation of the measurement system for Operational Risk (covering system and data used to calculate Operational Risk to estimate the capital charge for Operational Risk).**

	Bank calculates capital charges for operational risk using standardized approach starting year 2023 in accordance with regulatory requirement. Bank has RWA (Risk Weighted Asset) system to support in calculating capital charges for operational risk. Based on existing data sources, the RWA system will automatically calculate the capital charges for operational risk based on formula determined by the regulator based on business indicator components and historical operational risk loss data. The calculation result from the system can also be adjusted manually if necessary.
4	**Explanation of the scope and main coverage of the reporting framework for Operational Risk for executive officers and directors of the Bank.** Bank already has reports intended for Bank's executive officers (Board of Management) and Directors in monitoring operational risk both at Bank level and in the respective Directorates. At Bank level, operational risk reports will be submitted to the Directors and Executive Officers through the Risk Management Committee and to Board of Commissioners through the Risk Monitoring Committee. At the directorate level, operational risk reports will be submitted to the Directors and relevant executive officers through the quarterly RCM (Risk Control Meeting). Operational risk report submitted to Directors and Executive Officers but not limited to are: • Operational Risk Appetite (ORA) • operational risk and fraud event • Key Risk Indicators (KRI) • Results of Key Control Self-Assessment (KCSA) implementation
5	**Explanation of risk mitigation and risk transfer used in management for Operational Risk. This includes mitigation by issuing policies (such as policies for risk culture, risk acceptance, and outsourcing), by divesting high-risk businesses, and by establishing control functions. The remaining exposure can be absorbed by the Bank or for risk transfer. For example, the impact of operational losses can be mitigated by insurance.** In term of risk mitigation and risk transfer for Operational Risk Management, Bank has several risk control methods that are carried out at ongoing basis to ensure that every potential operational risk arising from business and operational activities is managed appropriately and does not exceed the acceptable limits. Several of risk mitigation and risk transfer method used are: • Identify and measure operational inherent risks in all work units. • Conduct operational risk reiew on new and developed products, services, systems and activities before being implemented to ensure adequate controls. • Ensure adequate policies and procedures to carry out every process and activity carried out in all business work units and supporting functions. • Conduct ongoing evaluations to assess the effectiveness of control adequacy and record and correct any deviations that occurs. • Conduct analysis in terms of risk transfer to transfer potential operational risks that may occur to other parties, such as through insurance protection. • Ensure the readiness of Business Continuity Management (BCM) for all critical work units.

RISK MANAGEMENT IMPLEMENTATION REPORT
FOR OPERATIONAL RISK

Bank Name: BTPN (consolidation)
Reporting Year: 2023 /(Audited)

1	**Explanation of regulations, policies and/or guidelines related to risk management for Operational Risk.** BTPN (hereinafter referred to as "Bank") and BTPN Syariah (hereinafter referred to as "BTPNS") as subsidiaries have policies and procedures for operational risk management. These policies and procedures are reviewed periodically with consider any changes in Bank and BTPNS's internal and external factors, especially related to to regulatory requirement. All work units in Bank and BTPNS must be guided by these policies and procedures in carrying out their daily operational activities. Policies and procedures related for Operational Risk Management are: • Operational Risk Management Policy • Business Continuity Management Policy • Insurance Management Policy • Information Security Management Policy • Key Control Self-Assessment (KCSA) procedure • Key Risk Indicator (KRI) procedure • Event Registration and Booking of Operational Risk (RLED) procedure • Significant Incident Notification Protocol (SINP) procedure • Operational & Fraud Risk Assessment (KROF) procedure • Internal Control and Risk (ICR) implementation procedure • Risk Grading Matrix (RGM) and Process Risk Control (PRC) procedure • Operational Risk Appetite (ORA) procedure • Risk Acceptance (RA) Procedure • Information Management and Security (POS) procedure • Risk Control Meeting (RCM) procedure • Business Impact Analysis (BIA) and Business Continuity Plan (BCP) procedure • Incident Management Plan (IMP) procedure • Initiative Management procedure • 2nd LoD Roles and responsibilities procedure • Anti Fraud Strategy procedure • Investigation procedure • Whistleblowing procedure • Fraud Reporting and Monitoring Procedure Policies and procedures related to Operational Risk Management in BTPNS are: • Operational Risk Management Policy • Business Continuity Management Policy • Anti Fraud Strategy Policy • Business Continuity Management Procedures • Business Impact Analysis Procedure • Business Continuity Plan procedure

	• Key Control Self-Assessment (KCSA) Procedure • Key Risk Indicator (KRI) procedure • Operational Risk Event Management Procedure • Quality Assurance (QA) Framework Procedure • Anti Fraud Strategy Procedure • Investigation Procedure • Whistleblowing Procedure
2	**Explanation of the structure and organization of management and control function related to Operational Risk.** Bank using 3 lines of defense model to divide the role and responsibilities of each party within the Bank's organization for the implementation of Operational Risk Management. **In the first line of defense,** all business and support functions work unit as risk owners who are directly responsible for the implementation of operational risk management. In its implementation, the work unit is supported by Business Risk. Besides supported by Business Risk, at the operational level Bank has ICR (Internal Control & Risk) function that responsible to support related work unit in managing their daily operational risk. The role and responsibilities of business and support functions work unit are: • Identify and register all operational inherent risks in each product, service, process, and initiative. • Record risk events and book operational risk losses and recovery. • Follow-up action for operational and fraud risk events and its completion. • Carry out all operational risk management program that has determined by OFRM Division. The role and responsibilities of the ICR (Internal Control & Risk) function are: • Act as coordinator in the implementation and completion of operational risk management implementation programs in their respective areas. • Assist work units in providing operational risk review. • Assist work units in issue resolution or operational risk events. • Conduct inspections and report each finding to the relevant parties. • Monitor follow-up action and resolution of each identified finding. **In the second line of defense,** is Operational & Fraud Risk Management (OFRM) Division which has direct reporting line to the Head of Risk Management, responsible for operational and fraud risk management. The roles and responsibilities of the OFRM Division are: • Create and develop operational and fraud risk management policies, procedures and tools. • Create operational and fraud risk management implementation programs. • Provide socialization and training on operational and fraud risk management to work units. • Support work units in providing operational and fraud risk review. • Create operational and fraud risk report to management and regulator. • Monitoring the implementation of operational and fraud risk management in Bank. • Create and develop ICRS (Internal Risk & Control system) as application used to manage operational risk in Bank. **In the third line of defense,** is Internal Audit to conduct inspection and evaluation of governance and implementation of operational risk management. Examination is carried out on the first line of defense and the second line of defense.

	The Board of Commissioners and Directors supervise the implementation of Operational Risk Management through the Risk Monitoring Committee and Risk Management Committee which are conducted regularly. The roles and responsibilities of the Board of Commissioners are: • Evaluate and approve policies and strategic plans for the implementation of operational and fraud risk management. • Monitor Operational Risk Appetite. • Provide direction on the implementation of operational and fraud risk management. The roles and responsibilities of Directors are: • Ensure the adequacy of the organizational structure and human resource for the implementation of operational risk management in their respective areas. • Ensure the implementation of operational risk management program has been carried out. • Monitor and ensure follow-up resolution of any operational issues or risk event and fraud event. • Develop awareness culture of operational and fraud risk. Similar with Bank, the adequacy of the structure and organization of management and control functions related to Operational Risk at BTPNS is carried out by separating the roles and responsibilities of work units by implementing the 3 line of defense model, namely: (First line of defense) units business work and support functions together with the Quality Assurance (QA) function ensure that activities are carried out in accordance with Bank policies and procedures. (Second line of defense), the Risk Management Work Unit (SKMR) carries out maintenance of the operational risk management methodology and ensures that BTPNS activities comply with regulatory provisions including compliance with sharia principles. (Third line of defense), Internal Audit ensures that all remaining risks (residual risks) are managed properly according to risk appetite & risk tolerance.
3	**Explanation of the measurement system for Operational Risk (covering system and data used to calculate Operational Risk to estimate the capital charge for Operational Risk).** Bank calculates capital charges for operational risk using standardized approach starting year 2023 in accordance with regulatory requirement. Bank has RWA (Risk Weighted Asset) system to support in calculating capital charges for operational risk. Based on existing data sources, the RWA system will automatically calculate the capital charges for operational risk based on formula determined by the regulator based on business indicator components and historical operational risk loss data. The calculation result from the system can also be adjusted manually if necessary. BTPNS as Sharia Bank, in accordance with OJK regulations is still calculating capital charges for operational risks using the Basic Indicator Approach. In the case of the need to calculate capital costs on a consolidated basis, the Bank will request business indicator data and historical operational risk loss data from BTPNS.
4	**Explanation of the scope and main coverage of the reporting framework for Operational Risk for executive officers and directors of the Bank.** Bank has reports intended for Bank's executive officers (Board of Management) and Directors in monitoring operational risk both at Bank level and in the respective Directorates. At Bank level, operational risk reports will be submitted to the Directors and Executive Officers through the Risk Management Committee and to Board of Commissioners through the Risk Monitoring Committee. At the directorate level, operational risk reports will be submitted to the Directors and relevant executive officers through the quarterly RCM (Risk Control Meeting). Operational risk report submitted to Directors and Executive Officers but not limited to are:

	• Operational Risk Appetite (ORA) • operational risk and fraud event • Key Risk Indicators (KRI) • Results of Key Control Self-Assessment (KCSA) implementation BTPNS also has reports intended for Bank's executive officers and Directors in monitoring operational risk. The data source used for preparing reports has been supported by the ORMS (Operational Risk Management System) application as database for recording operational risk events.
5	**Explanation of risk mitigation and risk transfer used in management for Operational Risk. This includes mitigation by issuing policies (such as policies for risk culture, risk acceptance, and outsourcing), by divesting high-risk businesses, and by establishing control functions. The remaining exposure can be absorbed by the Bank or for risk transfer. For example, the impact of operational losses can be mitigated by insurance.** In term of risk mitigation and risk transfer for Operational Risk Management, Bank has several risk control methods that are carried out at ongoing basis to ensure that every potential operational risk arising from business and operational activities is managed appropriately and does not exceed the acceptable limits. Several of risk mitigation and risk transfer method used are: • Identify and measure operational inherent risks in all work units. • Conduct operational risk reiew on new and developed products, services, systems and activities before being implemented to ensure adequate controls. • Ensure adequate policies and procedures to carry out every process and activity carried out in all business work units and supporting functions. • Conduct ongoing evaluations to assess the effectiveness of control adequacy and record and correct any deviations that occurs. • Conduct analysis in terms of risk transfer to transfer potential operational risks that may occur to other parties, such as through insurance protection. • Ensure the readiness of Business Continuity Management (BCM) for all critical work units.