Risk Exposure Publication Report – Operational

31 December 2022

I. Operational Risk Calculation

Quantitative Operational Risk Disclosure – Bank Stand Alone

(in million Rupiah)

No	Approach	31 December 2022			31 December 2021		
		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	8,624,711	1,293,707	16,171,334	8,688,851	1,303,328	16,291,596
	Total	8,624,711	1,293,707	16,171,334	8,688,851	1,303,328	16,291,596

Quantitative Operational Risk Disclosure – Consolidated Bank and Subsidiary

(in million Rupiah)

No	Approach	31 December 2022			31 December 2021		
		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	12,435,609	1,865,341	23,316,768	12,343,405	1,851,511	23,143,885
	Total	12,435,609	1,865,341	23,316,768	12,343,405	1,851,511	23,143,885

RISK MANAGEMENT IMPLEMENTATION REPORT
FOR OPERATIONAL RISK

Bank Name: BTPN (individual)
Reporting Year: 2022 /(un-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
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 and process. • Record operational risk events.

	• Develop follow-up plans for operational risk events and their resolution. • Implement all operational risk management implementation that have been programmed. The role and responsibilities of the ICR (Internal Control & Risk) function are: • Conduct inspection and report any operational risk findings to related parties. • Monitoring follow-up plans and settlement of any identified findings. **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 risk management and fraud policies, procedures, and tools. • Create operational risk management and fraud implementation program. • Provide socialization and training on operational risk management and fraud to work units. • Support work units in providing operational risk and fraud review. • Create operational risk and fraud reports to management and regulator. • Monitor the implementation of operational risk management and fraud in Bank. • Create and develop ICRS (Internal Risk & Control system) as application used for operational risk management 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 risk management. • Monitor Operational Risk Appetite. • Provide direction on the implementation of operational 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 risk issues or events. • Develop awareness culture of operational 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 in calculating capital charges for operational risk have used standardized approach which carried out for the first time in 2023 according to the OJK (Financial Services Authority) schedule and to replace the previous method of calculating capital charges with basic indicator approach. In making calculations, Bank already has system to support in calculating operational risk capital charges. The 2 data sources used are business indicator data and operational risk loss historical data which can be retrieved from the system automatically according to the required reporting period and manual adjustments can be made 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 events • 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 method 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: • Ensure the existence of policies and procedures to carry out all processes and activities in all business and support functions work unit. • Carry out ongoing evaluations to assess the effectiveness of the adequacy of controls and to record and correct any deviations that occurs. • Conduct analysis in terms of risk transfer to transfer potential operational risks that may occur ~~to~~ through insurance. • 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: 2022 /(un-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 in Bank 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 Policies and procedures related to Operational Risk Management in BTPNS are: • Operational Risk Management Policy • Business Continuity Management Policy • Key Control Self-Assessment (KCSA) procedure • Key Risk Indicator (KRI) procedure • Event Registration and Booking of Operational Risk (RLED) procedure • Risk Management Review Procedure • Quality Assurance (QA) Framework procedure • Technical Guidelines for Operational Risk Appetite & Tolerance
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 and process. • Record operational risk events. • Develop follow-up plans for operational risk events and their resolution. • Implement all operational risk management implementation that have been programmed. The role and responsibilities of the ICR (Internal Control & Risk) function are: • Conduct inspection and report any operational risk findings to related parties. • Monitoring follow-up plans and settlement of any identified findings. **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 risk management and fraud policies, procedures, and tools. • Create operational risk management and fraud implementation program. • Provide socialization and training on operational risk management and fraud to work units. • Support work units in providing operational risk and fraud review. • Create operational risk and fraud reports to management and regulator. • Monitor the implementation of operational risk management and fraud in Bank. • Create and develop ICRS (Internal Risk & Control system) as application used for operational risk management 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 risk management. • Monitor Operational Risk Appetite. • Provide direction on the implementation of operational 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 risk issues or events. • Develop awareness culture of operational 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 divide the role and responsibilities of work units by implementing the 3rd line of defense model, namely: (First line of defense) unit business work and support functions together with the Quality Assurance (QA) function ensure that the activities carried out are in accordance with the Bank's policies and procedures. (Second line of defense), the Risk Management Work Unit carries out maintenance of operational risk management methodologies and ensure that BTPNS activities comply with regulatory regulation including compliance with sharia principles. (Third line of defense), Internal Audit ensures that all remaining risks (residual risks) are properly managed 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 in calculating capital charges for operational risk have used standardized approach which carried out for the first time in 2023 according to the OJK (Financial Services Authority) schedule and to replace the previous method of calculating capital charges with basic indicator approach. In making calculations, Bank already has system to support in calculating operational risk capital charges. The 2 data sources used are business indicator data and operational risk loss historical data which can be retrieved from the system automatically according to the required reporting period and manual adjustments can be made if necessary. BTPNS as Sharia Bank, in accordance with OJK regulation is still calculating the capital charge for operational risk using the Basic Indicator Approach. For Consolidation purpose, Bank will request data on business indicator and historical data on operational risk losses to 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 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 events • 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 and BTPNS has several risk control method 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: • Identifying and measuring operational process and inherent risk in each work unit. • Conduct operational risk review on new product, services, systems and activities as well as enhancement before implemented to ensure adequate controls exist. • Ensure the policies and procedures for carrying out every process and activity in all business work units and support functions. • Carry out ongoing evaluations to assess the effectiveness of the adequacy of controls and to record and correct any deviations that occurs. • Conduct analysis in terms of risk transfer to transfer potential operational risks that may occur through insurance. • Ensure the readiness of Business Continuity Management (BCM) for all critical work units.