Risk Exposure Publication Report – Operational

30 June 2024

I. Operational Risk Calculation

Quantitative Operational Risk Disclosure – Bank Stand Alone

(in million Rupiah)

No	Approach	30 June 2023			30 June 2024		
		Business Indicator Component (average 3 years)	Capital Charge	RWA	Business Indicator Component (average 3 years)	Capital Charge	RWA
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
1	Standardized Approach	818,034.60	818,034.60	10,225,432.50	839,321.16	839,321.16	10,491,514.50
	Total	818,034.60	818,034.60	10,225,432.50	839,321.16	839,321.16	10,491,514.50

Quantitative Operational Risk Disclosure – Consolidated Bank and Subsidiary

(in million Rupiah)

No	Approach	30 June 2023			30 June 2024		
		Business Indicator Component (average 3 years)	Capital Charge	RWA	Business Indicator Component (average 3 years)	Capital Charge	RWA
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
1	Standardized Approach	840,067.33	840,067.33	10,500,841.63	858,358.43	858,358.43	10,729,480.38
	Total	840,067.33	840,067.33	10,500,841.63	858,358.43	858,358.43	10,729,480.38

RISK MANAGEMENT IMPLEMENTATION REPORT
FOR OPERATIONAL RISK

Bank Name: BTPN (individual)
Reporting Year: 2024 /(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 • Cyber Risk Management Policy • Anti Fraud Strategy 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 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 day to day operational risk. The role and responsibilities of business and support functions work unit are: • Identify and register all operational risks inherent in each product, service, process and initiative. • Recording operational risk event and bookkeeping operational risk losses and the recovery. • Develop action plan of operational risk event and fraud event and monitor the completion. • Carry out all operational risk management program made 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 follow up plan for operational risk incidents. • Conduct inspection and report findings to the relevant parties. • Monitor follow-up plan and completion 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 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. • Create and develop ICRS (Internal Risk & Control system) as an application used to manage operational risk at the 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 Commissioner and Board of Director 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 Commissioner 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 Board of Director 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 calculates capital charges for operational risk using a standardized approach starting in 2023 in accordance with regulatory provisions. The bank has RWA (Risk Weighted Asset) system to assist in calculating capital charges for operational risk. Based on existing data sources, the RWA system will automatically calculate capital charges for operational risks based on a formula determined by the regulator based on the product of business indicator components and historical operational risk loss data. The calculation results 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 Board of Director in monitoring operational risk both at Bank level and in the respective Directorates. At Bank level, operational risk reports will be submitted to the Board of Director and Executive Officers through the Risk Management Committee and to Board of Commissioners through the Risk Monitoring Committee. At the directorate level, operational risk report will be submitted to the Board of Director 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 Identify and measure the processes and operational inherent risks in each work unit. • Conduct operational risk review on new and developed products, services, systems and activities before they are marketed or implemented to ensure adequate controls. • Ensure that there are 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 occur. • 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: 2024 /(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 • Cyber Risk Management Policy • Anti Fraud Strategy 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 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 (Include BTPNS Ventura) are: • Operational Risk Management Policy • Business Continuity Management Policy • Anti Fraud Policy • 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 Policies and procedures related to Operational Risk Management in OTO&SOF are: • Guidelines for Implementing Anti-Fraud Strategy Policy • Business Quality Control Department policy • Risk Management Implementation Guidelines Policy • Guidelines for Implementing Risk Management in the Use of Information Technology Policy • Whistleblowing System Implementation Guidelines Policy • Business Continuity Plan (BCP) Policy • IT Disaster Recovery Plan (DRP) Policy • Security Operation Center (SOC) Policy • Risk Limit Determination Policy regarding Risk Management Implementation • Surveillance Policy • Policy regarding Changes in the number and Limit of Risk Appetite and Risk Tolerance in Key Risk Indicators (KRI)
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 day to day operational risk. The role and responsibilities of business and support functions work unit are: • Identify and register all operational risks inherent in each product, service, process and initiative. • Recording operational risk event and bookkeeping operational risk losses and the recovery. • Develop action plan of operational risk event and fraud event and monitor the completion. • Carry out all operational risk management program made 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 follow up plan for operational risk incidents. • Conduct inspection and report findings to the relevant parties. • Monitor follow-up plan and completion 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 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.
- Create and develop ICRS (Internal Risk & Control system) as an application used to manage operational risk at the 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 Commissioner and Board of Director 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 Commissioner 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 Board of Director 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.

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) business work units and support functions together with the Quality Assurance (QA) function ensures 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.

The adequacy of the structure and organization of management and control functions related to Operational Risk in OTO & SOF uses Three Lines of Defense, each unit work independently, namely:

The first line of defense, is business and operational functions (risk-taking function). Implemented by units/functions which are at the forefront of implementing Risk Management, with roles and responsibilities includes:

- Convey the inherent risk exposure (inherent risk) contained in each business and operational unit to the Risk Management function on a regular basis.
- Ensure that there is a conducive risk control environment in each business and operational unit.
- Implement established Risk Management policies in carrying out business and operational activities.
- Carry out recommendations from the Risk Management function in order to control risk in each business and operational unit.

The second line of defense, is the Risk Management function. Implemented by the Risk Management function/section in monitoring the implementation of the Risk Management strategy, with roles and responsibilities includes:

- Identifying risks including inherent risks in business activities.
- Develop risk measurement methods that are appropriate to the size and complexity of the business, including designing and implementing the tools needed to implement Risk Management.
- Monitoring the implementation of Risk Management strategies that have been approved by the Board of Directors, including monitoring Risk Management strategies in business and operational functions.
- Monitoring the overall Risk position (composite), per Risk type, and per type of functional activity against predetermined Risk tolerances and limits.
- Conduct regular reviews of the Risk Management process.
- Prepare and submit Risk profile reports to the Board of Directors in charge of the Risk Management function and Risk Management committee on regular basis, where the frequency of reports can be increased if market conditions change rapidly.

The third line of defense is the internal control function or internal audit function. Implemented by the Internal Audit Work Unit (SKAI), with roles and responsibilities includes:

- Ensure compliance at all levels of the Company's organization with established Risk Management policies and procedures.
- Ensure that the effectiveness of the implementation of Risk Management is in accordance with the Risk Management strategy and policy.
- Ensure the effectiveness of the Risk culture in the Company as a whole.

The Board of Director and Board of Commissioner are responsible for the effectiveness of the implementation of Risk Management by supervising the implementation of Risk Management through the Risk Monitoring Committee and the Risk Management Committee which are carried out periodically.

The roles and responsibilities of the Board of Directors & Board of Commissioners include:

- The Board of Director and Board of Commissioner must ensure that the implementation of Risk Management for Operational Risk is carried out effectively and is integrated with the implementation of Risk Management for other areas which may have an impact on the overall Risk profile.
- The Board of Director and Board of Commissioner are responsible for developing an organizational culture that is aware of Operational Risk and fosters commitment to managing Operational Risk in accordance with business strategy.
- The Board of Director creates a culture of objective disclosure of Operational Risks to all elements of the organization so that Operational Risks can be identified quickly and mitigated appropriately.
- The Board of Director ensures that it establishes a reward policy including effective remuneration and punishment that is integrated into the performance assessment system in order to support optimal implementation of Risk Management.
- The Board of Director must ensure that the implementation of authority and responsibility transferred to service providers has been carried out properly and responsibly.

	• The Board of Commissioners ensures that the remuneration policy is in accordance with the Risk Management strategy.
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 a standardized approach starting in 2023 in accordance with regulatory provisions. The bank has RWA (Risk Weighted Asset) system to assist in calculating capital charges for operational risk. Based on existing data sources, the RWA system will automatically calculate capital charges for operational risks based on a formula determined by the regulator based on the product of business indicator components and historical operational risk loss data. The calculation results from the system can also be adjusted manually 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. OTO and SOF as finance companies are not yet required by the regulator to calculate capital charges for operational risks.
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 Board of Director in monitoring operational risk both at Bank level and in the respective Directorates. At Bank level, operational risk reports will be submitted to the Board of Director and Executive Officers through the Risk Management Committee and to Board of Commissioners through the Risk Monitoring Committee. At the directorate level, operational risk report will be submitted to the Board of Director 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 executive officers and Bank Directors in monitoring operational risks. The data source used to create the report is supported by the ORMS (Operational Risk Management System) application as a database for recording operational risk events. And currently BTPNS Risk Management is developing a new system, namely ORBAS (Operational Risk Based System), which will later replace ORMS, with plans to implement phase 1 at the end of 2024. OTO and SOF as finance companies also have reports to the Board of Directors in monitoring operational risks.
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 subsidiaries 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 Identify and measure the processes and operational inherent risks in each work unit. • Conduct operational risk review on new and developed products, services, systems and activities before they are marketed or implemented to ensure adequate controls. • Ensure that there are 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.