Risk Exposure Publication Report – Operational

30 June 2025

Operational Risk Calculation

Quantitative Operational Risk Disclosure – Bank Stand Alone

(in million Rupiah)

No	Approach	30 June 2025			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	839.546	839.546	10.494.328	839.321	839.321	10.491.514
	Total	**839.546**	**839.546**	**10.494.328**	**839.321**	**839.321**	**10.491.514**

Quantitative Operational Risk Disclosure – Consolidated Bank and Subsidiary

(In million Rupiah)

No	Approach	30 June 2025			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	900.340	900.340	11.254.250	858.358	858.358	10.729.480
	Total	**900.340**	**900.340**	**11.254.250**	**858.358**	**858.358**	**10.729.480**

RISK MANAGEMENT IMPLEMENTATION REPORT
FOR OPERATIONAL RISK

Bank Name: PT Bank SMBC Indonesia Tbk (individual)
Reporting Year: 2025 /(Audited)

1	**Explanation of regulations, policies and/or guidelines related to risk management for Operational Risk.** PT Bank SMBC Indonesia Tbk (SMBC Indonesia) 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 • Third Party Risk Management Policy • Internal Control Policy Over Financial Information And/Or Financial Report • Cyber Risk Management Policy • Conduct 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 • Non Financial 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 • Internal Control Procedure Over Financial Information And/Or Financial Report
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 supporting function work unit as the risk owners are directly responsible for the implementation of operational risk management. In its implementation, each work units has Business Risk/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 measure all potential operational inherent risks in each product, service, process and initiative • Record risk events and bookkeeping of operational risk/fraud losses and recovery • Prepare follow-up action for operational risk/fraud risk event and monitor its completion • Implement all operational risk management and Anti-Fraud Strategy program set by OFRM Division The role and responsibilities of the ICR (Internal Control & Risk) function are: • Act as a coordinator in the implementation and completion of operational risk management program in their respective areas • Support work unit in providing review on operational risk and fraud • Support work unit in completion and action plan on operational risk/fraud issues or events • Conduct inspection on the adequacy of control over each process carried out in their respective areas and report any findings to relevant parties • Monitor follow-up action and resolution of each operational risk/fraud issue or event • As PIC to coordinate with the OFRM Division and Internal Audit and other related work units in the implementation of operational risk management **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 Anti Fraud Strategy policies, procedures and tools. • Create operational risk management and Anti Fraud Strategy implementation programs. • Provide socialization and training on operational risk management and Anti Fraud Strategy 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 risk management and Anti Fraud Strategy 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,** Internal Audit conduct inspection and evaluation of the overall governance and implementation of operational risk management. conduct inspection and evaluation are conducted on the first line of defense and also the second line of defense. The Board of Commissioners and the Board of Directors supervise the implementation of Operational Risk Management. The Board of Commissioners through the Risk Monitoring Committee and the Board of Directors through the Risk Management Committee or Non-Financial Risk Management Committee which is conducted periodically in accordance with the applicable Charter. The roles and responsibilities of the Board of Commissioners are: • Evaluate and approve policies and strategic plans for the implementation of operational risk management and Anti Fraud Strategy • Monitor Operational Risk Appetite • Provide direction on the implementation of operational risk management and Anti Fraud Strategy 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 and Anti Fraud Strategy program has been carried out • Monitor the implementation of operational risk management and ensure follow-up resolution of any issues/operational risk event/fraud • Develop awareness culture of operational risk and Anti Fraud 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 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 has reports addressed to the BoM (Board of Management) and the Bank's Directors in monitoring operational risks both at the Bank level and at the respective Directorates. The data sources in making these reports are mostly supported by the ICRS (Internal Control & Risk System)

	application owned by Bank which functioned as central database and is also used for operational risk management in all work units. At the Bank level, discussions regarding operational risks will be submitted to the Board of Directors and BoM through the Risk Management Committee and/or Non-Financial Risk Management Committee and to the Board of Commissioners through the Risk Monitoring Committee. At the Directorate level, discussions on operational risks will be submitted to the relevant Board of Director/BoM and Division Head in the relevant Directorate through the RCM (Risk Control Meeting) which is held quarterly. The discussions on operational risk submitted through the Risk Management Committee, Non Financial Risk Management Committee and Risk Monitoring Committee are as follows (but not limited to): • Non Financial Risk Appetite • Operational risk/fraud events along with losses and recovery • Key Risk Indicators (KRI) • Risk Acceptance • Top & Emerging Risk (Non Financial Risk) • Results of the implementation of Key Control Self-Assessment (KCSA)
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: • Identifying and measuring operational inherent risks in all work units. • Conduct operational risk and fraud risk review on products, services, systems and initiatives, both new and development, 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. • Conducting risk transfer analysis to transfer potential operational risks that may occur to other parties, such as through insurance protection • Conducting screening & due diligence processes for each implementation of cooperation carried out by the Bank with third parties (Business Partners and Vendors) • Ensuring the readiness of Business Continuity Management (BCM) for all critical work units

RISK MANAGEMENT IMPLEMENTATION REPORT
FOR OPERATIONAL RISK

Bank Name: PT Bank SMBC Indonesia Tbk (consolidated)
Reporting Year: 2025 /(Audited)

1	**Explanation of regulations, policies and/or guidelines related to risk management for Operational Risk.** PT Bank SMBC Indonesia Tbk (hereinafter referred to as "Bank") as the parent company along with BTPN Syariah (hereinafter referred to as "BTPNS"), PT Oto Multiartha (hereinafter referred to as "OTO") and PT Summit Oto Finance (hereinafter referred to as "SOF") as subsidiaries have policies and procedures for operational risk management. These policies and procedures are reviewed periodically with consider any changes in internal Bank and external factors, especially related to to regulatory requirement. All work units in Bank and subsidiaries 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 • Third Party Risk Management Policy • Internal Control Policy Over Financial Information And/Or Financial Report • Cyber Risk Management Policy • Conduct 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 • Non Financial 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 • Internal Control Procedure Over Financial Information And/Or Financial Report 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 • *Process Risk Control (PRC) 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 at OTO SOF include: • Policy on Guidelines for Implementing Anti-Fraud Strategy • Policy on Implementing Anti-Bribery/Gratification and Corruption • Policy on Declaration of Anti-Bribery/Gratification and Corruption • Policy on Investment Committee • Policy on Guidelines for Implementing Anti-Money Laundering, Prevention of Terrorism Funding, and Prevention of Funding for Proliferation of Weapons of Mass Destruction • Policy on Business Quality Control Department • Policy on Guidelines for Implementing Risk Management • Policy on Guidelines for Implementing Risk Management in the Use of Information Technology • Policy on Guidelines for Implementing Whistleblowing System • Policy on Business Continuity Plan (BCP) • Policy on IT Disaster Recovery Plan (DRP) • Policy on Security Operation Center (SOC) • Policy on Determining Risk Limits in the Framework of Implementing Risk Management • Policy on Surveillance • Policy on Changes in the Amount and Limit of Risk Appetite and Risk Tolerance on Key Risk Indicators (KRI)

	• Policy on Guidelines for Recording Incidents and Accounting for Operational Risks
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 supporting function work unit as the risk owners are directly responsible for the implementation of operational risk management. In its implementation, each work units has Business Risk/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 measure all potential operational inherent risks in each product, service, process and initiative • Record risk events and bookkeeping of operational risk/fraud losses and recovery • Prepare follow-up action for operational risk/fraud risk event and monitor its completion • Implement all operational risk management and Anti-Fraud Strategy program set by OFRM Division The role and responsibilities of the ICR (Internal Control & Risk) function are: • Act as a coordinator in the implementation and completion of operational risk management program in their respective areas • Support work unit in providing review on operational risk and fraud • Support work unit in completion and action plan on operational risk/fraud issues or events • Conduct inspection on the adequacy of control over each process carried out in their respective areas and report any findings to relevant parties • Monitor follow-up action and resolution of each operational risk/fraud issue or event • As PIC to coordinate with the OFRM Division and Internal Audit and other related work units in the implementation of operational risk management **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 Anti Fraud Strategy policies, procedures and tools. • Create operational risk management and Anti Fraud Strategy implementation programs. • Provide socialization and training on operational risk management and Anti Fraud Strategy 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 risk management and Anti Fraud Strategy 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, Internal Audit conduct inspection and evaluation of the overall governance and implementation of operational risk management. conduct inspection and evaluation are conducted on the first line of defense and also the second line of defense.

The Board of Commissioners and the Board of Directors supervise the implementation of Operational Risk Management. The Board of Commissioners through the Risk Monitoring Committee and the Board of Directors through the Risk Management Committee or Non-Financial Risk Management Committee which is conducted periodically in accordance with the applicable Charter.

The roles and responsibilities of the Board of Commissioners are:

- Evaluate and approve policies and strategic plans for the implementation of operational risk management and Anti Fraud Strategy
- Monitor Operational Risk Appetite
- Provide direction on the implementation of operational risk management and Anti Fraud Strategy

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 and Anti Fraud Strategy program has been carried out
- Monitor the implementation of operational risk management and ensure follow-up resolution of any issues/operational risk event/fraud
- Develop awareness culture of operational risk and Anti Fraud Strategy

Adequacy of 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.

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 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. 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 has reports addressed to the BoM (Board of Management) and the Bank's Directors in monitoring operational risks both at the Bank level and at the respective Directorates. The data sources in making these reports are mostly supported by the ICRS (Internal Control & Risk System) application owned by Bank which functioned as central database and is also used for operational risk management in all work units. At the Bank level, discussions regarding operational risks will be submitted to the Board of Directors and BoM through the Risk Management Committee and/or Non-Financial Risk Management Committee and to the Board of Commissioners through the Risk Monitoring Committee. At the Directorate level, discussions on operational risks will be submitted to the relevant Board of Director/BoM and Division Head in the relevant Directorate through the RCM (Risk Control Meeting) which is held quarterly.

	The discussions on operational risk submitted through the Risk Management Committee, Non Financial Risk Management Committee and Risk Monitoring Committee are as follows (but not limited to): • Non Financial Risk Appetite • Operational risk/fraud events along with losses and recovery • Key Risk Indicators (KRI) • Risk Acceptance • Top & Emerging Risk (Non Financial Risk) • Results of the implementation of Key Control Self-Assessment (KCSA) BTPNS also has reports intended for Directors, BoM and Division Head 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. 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 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: • Identifying and measuring operational inherent risks in all work units. • Conduct operational risk and fraud risk review on products, services, systems and initiatives, both new and development, 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. • Conducting risk transfer analysis to transfer potential operational risks that may occur to other parties, such as through insurance protection • Conducting screening & due diligence processes for each implementation of cooperation carried out by the Bank with third parties (Business Partners and Vendors) • Ensuring the readiness of Business Continuity Management (BCM) for all critical work units