



Summary of Risk Management Policy PT Bank CIMB Niaga Tbk

The Policy is effective since obtain approval from the Board of Commissioner (BoC) in May 2018

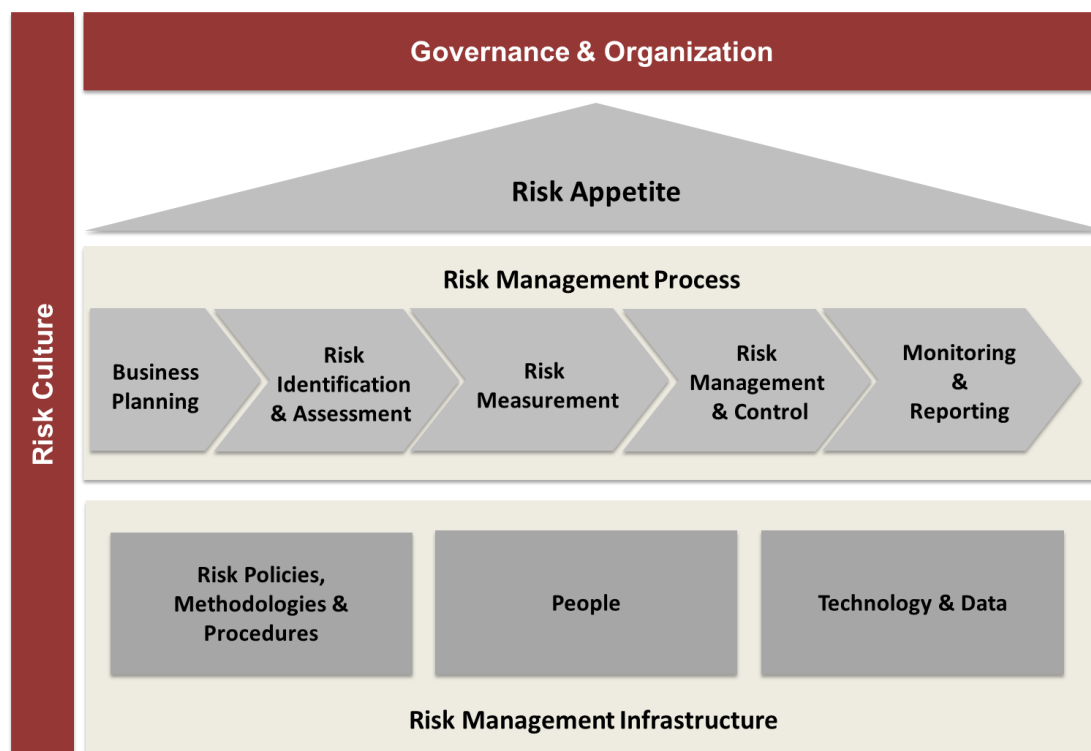
Risk management is an essential part of operational activities and decision making process in order to achieve business objectives. Risk management is actively implemented to maximize value added for the shareholders, manage capital comprehensively and maintain sound capital level, as well as ensure sustainable profitability and business growth. The Bank employs the Enterprise Wide Risk Management (EWRM) framework or policy to manage its risks on integrated view through risk appetite and business strategy alignment.

The policy is a standardized guideline to manage and anticipate both the existing and potential risks, taking into consideration the changing risk profiles as dictated by changes in business strategies, external environments and regulatory environment. The risks monitored periodically and the whole risk management process is conducted based on Good Corporate Governance principles implementation. The policy applies to all units including Syariah Banking and become guideline on risk management implementation in subsidiary and affiliated companies in accordance with OJK regulation.

Enterprise Wide Risk Management (EWRM) Framework

The EWRM Framework provides guideline for all internal stakeholders to manage its risks and become reference for external stakeholders to assess risk management implementation in CIMB Niaga, subsidiary and affiliated companies.

The main objective of EWRM is to ensure the Bank business activities are protected against losses which may threaten business sustainability. This framework also refers to the risk management scopes determined by The Financial Services Authority (OJK) which are (1) Active supervision of the Board of Commissioners (BoC) and the Board of Directors (BoD), (2) Policies, procedures and limit setting adequacy, (3) Risk identification, measurement, monitoring and controlling as well as risk management information system adequacy, and (4) Comprehensive internal control system.



- *EWRM Framework* components are as follows:

i) Risk Culture

The Bank embraces risk management as an integral part of corporate culture and decision-making processes. The risk management philosophy is embodied in the Three Lines of Defense approach in which risks are managed at the point of risk-taking activity. There is clear accountability of risk ownership across units in the Bank.

Line 1: Risk Taking Unit (Business Unit and Support Unit)

The first line is line management, both from business units and support units. These units deal with risks on daily activity, hence they are in the most appropriate position to manage risks and ensure compliance with regulations, standards, policies and procedures. In the risk management process, these units are the first line of defense to manage risks including but not limited to the process of identifying, measuring, monitoring, controlling and reporting risks as well as taking appropriate actions to mitigate risks to ensure they are “in control” position.

Line 2: Risk Management, Compliance and Anti Fraud Management Unit

The second line of defense is in charge to perform an independent oversight function of business activities and reporting to management in order to ensure the Bank is conducting business and operating in accordance with the appetite and regulatory requirements. The second lines are including risk management, compliance and anti

fraud management unit. These units in conjunction with business units ensure that each risk has been properly identified and managed. These second line units also develop strategies, implement policies and procedures and compile information to gain holistic view of the Bank risks.

Line 3: Internal Audit Unit

The third line of defense is Internal Audit unit which is an independent unit that directly responsible to the CEO and functionally to the BoC through Audit Committee. The scope of Internal Audit function is to evaluate risk management implementation and control process in the Bank such as whether the risks have been properly identified and managed and the quality and continuous improvement has been embedded in the Bank control process, both on the first line and the second line.

ii) Governance & Organization

In order to implement effective risk management, the Bank and other financial conglomerate member entities should establish an organizational structure which aligned with business objectives and policies, size and complexity as well as the inherent risk.

In the risk management process, strong corporate governance structure is required to improve four eyes principle mechanism and transparency, hence the effectiveness and consistency of EWRM Framework implementation could be achieved. Regarding risk management implementation, the BoC, Sharia Supervisory Board (DPS) and BoD are assisted by the respective committees to ensure objectivity and decision-making quality.

Effective oversight functions to be performed by BoC are as follows:

1. Approve and evaluate risk management directions, policies and strategies, at least once a year or more if there are significant changes on the factors affecting the Bank's business activities. Risk management policies and strategies should consider the impact on the Bank's capital.
2. Evaluate BoD accountability on risk management policy implementation at least on quarterly basis.
3. Evaluate and take decision on BoD's application or proposal related to transactions or business activities which required BoC approval.
4. Supervise BoD accountability on risk management external reporting.
5. Ensure integrated risk management implementation as part of conglomeration that includes at least point 1 and 2 above.

To assist BoC in ensuring the execution of oversight and consultative function for BoD as well as compliance with the internal and external regulations, the Bank established Risk Monitoring Committee (KIPER). BoD assisted by risk committees and control function in order to ensure the effectiveness of EWRM Framework implementation. The Committees generally making decisions regarding risk management directions and policies according to their respective functions including Risk Management Committee, Assets and Liabilities Committee (ALCO), Credit Policy Committee (CPC), and Operational Risk Committee (ORC). The Bank also established Integrated Risk Management Committee in regards to integrated risk management implementation.

At operational level, in addition to Risk Management Unit, other units involved in internal control functions are Compliance, Anti Fraud Management (AFM) and Syariah Advisory. Besides, independent reviews are periodically conducted by Internal Audit, Risk Model Validation and Credit Assurance Testing.

iii) Risk appetite

Risk Appetite is defined as the types and amount of risks that the Bank is able and willing to accept in pursuit of its strategic and business objectives. Risk Appetite is dynamic, evolving in response to changes in the Bank business priorities, risk management capabilities and external conditions. Risk appetite takes into account not only growth, revenue and business aspirations, but also the capital and liquidity positions and risk management capabilities and strengths, including risk systems, processes and people.

The objective of Risk Appetite framework is to ensure that the boundaries of acceptable risk-taking are fully aligned with the Bank's strategy and business operating plans and also sufficiently clear to guide the senior and front-line employees in all of the business units in their day-to-day decision-making. The process for risk appetite is conducted on annual basis.

The Risk Appetite Statements (RAS) has 4 measurement categories that link business target, risk level and capital. RAS is presented in quantitative and qualitative analysis which includes: (i) Solvency and capitalization (ii) Earning diversification and volatility (iii) Liquidity and (iv) Franchise.

The Bank Risk Appetite reflects risk management capabilities and strengths, including systems, processes and people. The Bank will at all times aim to ensure that its risk systems, capabilities and controls are sufficiently resourced and effective to underpin its desired risk appetite, through accurate risk identification and measurement.

iv) Risk Management Process

The aim of good risk management process is to address the risk attached the Bank's activities in order to add maximum sustainable value to all activities of the organizations. Risk management process is employed as part of daily activities, with the goal of ensuring risks are appropriately considered, evaluated and responded in a timely manner.

a. Business Planning

Risk management is central to the business planning process as part of daily operations. Integration of risk management into business planning helps to ensure that Bank operates within the approved Risk Appetite.

b. Risk Identification and Assessment

For effective risk management, risks must be clearly defined, proactively identified and assessed on an ongoing and forward looking basis. Proper risk identification and assessment focuses on recognizing and understanding all key risks inherent in our business activities or key risks that may arise from external factors or uncertainties.

Risk types that are recognized by the Bank also refer to OJK's regulation, which includes main risks namely, credit risk, market risk, liquidity risk, operational risk, legal risk, reputation risk, strategic risk, compliance risk, intragroup transaction and insurance risk (if any), for UUS, it also covers 2 (two) syariah's specific risks, namely rate of return risk and investment risk. These risk types can be differ according to changes on regulations or Bank's complexity and business characteristic going forward, based on assessments and reviews conducted by business unit and risk management.

Bank identified risks through *Risk & Control Self Assessment (RCSA)* and *Risk Assessment*. *RCSA* is a structured approach that enables the first line of defense to identify and assess the key risks and controls in order to plan for appropriate actions to minimize the exposure of those risks.

Risk Assessment includes risk identification and assessment as follows:

1. Annual assessment of risk which categorized as non Pilar 1 and risks which capital requirements can't be quantified/ measured. Risk identification is performed by business units and selective support units that are responsible to manage certain risk types. This process is part of *Internal Capital Adequacy Assessment Process (ICAAP)* to assess Bank's capital adequacy.

2. On going *Risk Assessment* process that is carried out simultaneously as part of business as usual activity. That activity for instance is conducted during evaluation of new business segments, new product approval and policy & procedures periodic review.

c. Risk Measurement

Risk measurement aims to measure Bank's risk profile to portray the effectiveness of risk management implementation by knowing the risk of products, portfolios and activities, as well as the impact towards Bank's profitability and capital. Risk loss measurement is very crucial for provisioning and sound capital adequacy. Risk measurement is conducted by using tools (methodologies, models, etc) across each of the risk types through quantitative and qualitative approach, based on reference and best practice in financial and banking industry, including *stress testing*. In conducting risk measurement, Bank must, at minimum: (i) evaluate the relevance of assumption, data source and procedure used to measure risk periodically and (ii) enhancement on risk measurement system if there are changes on Bank's business activities, products, transactions and risk factors that are material.

d. Risk Management and Control

Managing and mitigating risk are an integral part of the Bank's business, which aim to reduce the risk to a level which is manageable. This can be achieved through utilizing various control tools to reduce the likelihood of an occurrence or the impact of the risk. In general, several ways to manage and mitigate risks are *accept risk, treat risk, transfer risk* and *terminate risk*.

If the Bank decides to consciously *accept* or *treat* the risk, risk management limit and control must be established to manage the risk. Limit allows management to control exposures and monitor actual risk taking against predetermined tolerances. Risk management limit and control is monitored and reviewed periodically to align with business needs, market condition and regulatory changes.

e. Monitoring and Reporting

Risk monitoring allows Bank to evaluate risk exposure simultaneously and improve reporting process if there are material changes on the Bank's business activities, products, transactions, risk factors, information technology and risk management information system.

Risk Taking Unit's activity is reported on periodic basis to ensure that risk exposures, both at individual and portfolio level are within Bank's risk appetite. Those reports help management for risk monitoring and taking business decisions.

v) Risk Management Infrastructure

An effective risk management infrastructure is critical to effective *enterprise wide risk management*. Main aims of an effective risk management infrastructure include providing an integrated view of risk from across the organization; reduce inefficiencies and redundancies, drives consistent treatment of risks across the organization, creating "risk aware" thinking and decision making at all levels, and enables appropriate flows of risk information up, down and across the organization.

Risk Management implementation must be supported by several infrastructures, namely:

a. Risk Policies, Methodologies and Procedures

Well defined risk management policy across risk types provides principles for the Bank to manage the risk. Methodologies provides subject specific requirements to be met to comply with the policy. Procedures provide more detailed instructions to assist with the implementation of policies. Policies, methodologies or standard, and procedures enable unified view of risk across the organization, including standardized risk definitions and common risk language.

b. People

Attracting the right talent and skills are the key to ensuring a well functioning *EWRM Framework*. Organization changes simultaneously and proactively to respond the increasing complexity of Bank's environment and regulation.

Performance and compensation measurement is aligned with strategic plan and risk appetite. The objectives of risk based performance are to:

- i) To provide management with comprehensive view of capital management because this concept linked Bank's strategic planning to the risks that are undertaken.
- ii) To optimize the returns of the Bank vis-à-vis available capital and underlying risks.
- iii) Support Bank's management in early detection of future expected loss.
- iv) As part of consideration of business unit's performance measurement, especially in setting the right compensations and incentives.

Risk based performance measurement concept will continuously improved and enhances aligned with Bank's capability in terms of methodology, information system, infrastructure and available resources.

c. Data and Technology

Appropriate technology and sound data management support risk management activities. To enhance the effectiveness of risk measurement process, Bank must have information system that provides timely and accurate report and data that support management decision making.

Bank's risk management information system can ensure:

- a. Ability to measure risk exposure accurately, informatively and in a timely manner, both composite risk exposure and exposure for each risk types that are inherent to Bank's business activities, and risk exposure for each functional activities.
- b. Compliance of risk management implementation to policy, procedure and risk limit;
- c. Availability of result (realization) of risk management implementation as compared to Bank's predetermined target based on risk management policy and strategy.

Information system must be able to provide report as a tool for continuous risk monitoring in order to detect and resolve deviation towards policies and procedures in a timely manner to reduce the potential loss events.