INDUSTRIAL AND COMMERCIAL BANK OF CHINA (CANADA)

BASEL III PILLAR 3 DISCLOSURES

AS AT DECEMBER 31, 2024

Table of Contents

Notes to Users

This document addresses the Basel III Pillar 3 disclosure requirements for Industrial and Commercial Bank of China (Canada) (the "Bank") in accordance with *OSFI's Pillar 3 Disclosure Guideline for Small and Medium-Sized Deposit-Taking Institutions (SMSBs) Capital and Liquidity Requirements* (the "Guideline") https://www.osfi-bsif.gc.ca/en/guidance/guidance-library/pillar-3-disclosure-guideline-small-medium-sized-deposit-taking-institutions-smsbs-guideline-2024

The following disclosures do not constitute any form of financial statements and must not be relied upon in making any investment or judgment on the Bank or its shareholder bank.

Segmentation Category

The Bank is currently categorized as Category 2 SMSB in accordance with *OSFI's Small and Medium-Sized Deposit-Taking Institutions (SMSBs) Capital and Liquidity Requirements,* section entitled "Segmentation of SMSBs"
https://www.osfi-bsif.gc.ca/Eng/fi-if/rg-ro/gdn-ort/gl-ld/Pages/SMSB.aspx#ToC3.0.

Financial Data Website

For the Bank's Financial Data, refer to OSFI's Financial Data for Banks website https://www.osfi-bsif.gc.ca/Eng/wt-ow/Pages/fd-df.aspx

Frequency of Reporting

OSFI expects SMSBs to adhere to the Guideline for frequency and format of reporting. Accordingly, the Bank's relevant quantitative disclosure are provided quarterly, and the general qualitative information of credit risk and operational risk are provided annually, at year-end.

Key Metrics

Key Metrics –KM1

	Item	Amounts (CAD in '000 except ratios)				
		Dec 31, 2024	**Sep 30, 2024**	**Jun 30, 2024**	**Mar 31, 2024**	**Dec 31, 2023**
	Available capital (amounts)					
1	Common Equity Tier 1 (CET1)	484,977	480,048	473,287	464,353	445,740
2	Tier 1	484,977	480,048	473,287	464,353	445,740
3	Total capital	513,148	504,740	497,864	488,835	479,580
	Risk-weighted assets (amounts)					
4	Total risk-weighted assets (RWA)	3,043,880	2,767,698	2,734,135	2,599,221	2,833,021
4a	Total risk-weighted assets (pre-floor)	3,043,880	2,767,698	2,734,135	2,599,221	2,833,021
	Risk-based capital ratios as a percentage of RWA					
5	CET1 ratio (%)	15.93%	17.34%	17.31%	17.87%	15.73%
5a	CET1 ratio (%) (pre-floor ratio)	15.93%	17.34%	17.31%	17.87%	15.73%
6	Tier 1 ratio (%)	15.93%	17.34%	17.31%	17.87%	15.73%
6a	Tier 1 ratio (%) (pre-floor ratio)	15.93%	17.34%	17.31%	17.87%	15.73%
7	Total capital ratio (%)	16.86%	18.24%	18.21%	18.81%	16.93%
7a	Total capital ratio (%) (pre-floor ratio)	16.86%	18.24%	18.21%	18.81%	16.93%
	Additional CET1 buffer requirements as a percentage of RWA					
8	Capital conservation buffer requirement (2.5% from 2019) (%)	2.50%	2.50%	2.50%	2.50%	2.50%
9	Countercyclical buffer requirement (%)	0	0	0	0	0
11	Total of bank CET1 specific buffer requirements (%) (row 8 + row 9)	2.50%	2.50%	2.50%	2.50%	2.50%
12	CET1 available after meeting the bank's minimum capital requirements (%) *	11.43%	12.84%	12.81%	13.37%	11.23%
	Basel III Leverage ratio					
13	Total Basel III leverage ratio exposure measure	3,713,809	3,474,203	3,410,396	3,244,559	3,588,112
14	Basel III leverage ratio (row 2 / row 13)	13.06%	13.82%	13.88%	14.31%	12.42%

*Calculated as row 5 minus minimum CET1 requirement of 4.5%

Composition of Capital

Composition of regulatory capital -Modified CC1

Q4 2024 as at Dec 31, 2024

	Item	Amounts (CAD in '000 except ratios)
	Common Equity Tier 1 capital: instruments and reserves	
1	Directly issued qualifying common share capital (and equivalent for non-joint stock companies) plus related stock surplus	208,000
2	Retained earnings	276,630
3	Accumulated other comprehensive income (and other reserves)	348
4	Directly issued capital subject to phase out from CET1 (only applicable to Federal Credit Unions)	-
5	Common share capital issued by subsidiaries and held by third parties (amount allowed in group CET1)	-
6	**Common Equity Tier 1 capital before regulatory adjustments**	484,978
	Common Equity Tier 1 capital: regulatory adjustments	
28	**Total regulatory adjustments to Common Equity Tier 1**	(1)
29	**Common Equity Tier 1 capital (CET1)**	484,977
	Additional Tier 1 capital: instruments	
36	**Additional Tier 1 capital before regulatory adjustments**	-
	Additional Tier 1 capital: regulatory adjustments	
43	**Total regulatory adjustments to additional Tier 1 capital**	-
44	**Additional Tier 1 capital (AT1)**	-
45	**Tier 1 capital (T1 = CET1 + AT1)**	484,977
	Tier 2 capital: instruments and provisions	
50	Collective allowances	28,171
51	**Tier 2 capital before regulatory adjustments**	28,171
	Tier 2 capital: regulatory adjustments	
57	**Total regulatory adjustments to Tier 2 capital**	-
58	**Tier 2 capital (T2)**	28,171
59	**Total capital (TC = T1 + T2)**	513,148
60	**Total risk-weighted assets**	3,043,880
	Capital ratios	
61	Common Equity Tier 1 (as a percentage of risk-weighted assets)	15.93%
62	Tier 1 (as a percentage of risk-weighted assets)	15.93%
63	Total capital (as a percentage of risk-weighted assets)	16.86%
	OSFI target	
69	Common Equity Tier 1 target ratio	7.00%
70	Tier 1 capital target ratio	8.50%
71	Total capital target ratio	10.50%

Leverage Ratio

Leverage Ratio -LR2

	Item	Amounts (CAD in '000 except ratios)	
		Dec 31,2024	**Sept 30,2024**
On-balance sheet exposures			
1	On-balance sheet items (excluding derivatives, SFTs and grandfathered securitization exposures but including collateral)	3,124,966	2,878,609
2	Gross-up for derivatives collateral provided where deducted from balance sheet assets pursuant to the operative accounting framework (IFRS)	(2,470)	(2,232)
3	(Deductions of receivable assets for cash variation margin provided in derivatives transactions)	(6,069)	(5,704)
4	(Asset amounts deducted in determining Tier 1 capital)	(1)	(2)
5	**Total on-balance sheet exposures (excluding derivatives and SFTs) (sum of lines 1 to 4)**	3,116,426	2,870,671
Derivative exposures			
6	Replacement cost associated with all derivative transactions	3,458	3,124
7	Add-on amounts for potential future exposure associated with all derivative transactions	3,849	2,419
8	(Exempted central counterparty-leg of client cleared trade exposures)	-	-
9	Adjusted effective notional amount of written credit derivatives	-	-
10	(Adjusted effective notional offsets and add-on deductions for written credit derivatives)	-	-
11	**Total derivative exposures (sum of lines 6 to 10)**	7,307	5,543
Securities financing transaction exposures			
12	Gross SFT assets recognized for accounting purposes (with no recognition of netting), after adjusting for sale accounting transactions	-	-
13	(Netted amounts of cash payables and cash receivables of gross SFT assets)	-	-
14	Counterparty credit risk (CCR) exposure for SFTs	-	-
15	Agent transaction exposures	-	-
16	**Total securities financing transaction exposures (sum of lines 12 to 15)**	-	-
Other off-balance sheet exposures			
17	Off-balance sheet exposure at gross notional amount	1,406,782	1,432,215
18	(Adjustments for conversion to credit equivalent amounts)	(816,706)	(834,226)
19	**Off-balance sheet items (sum of lines 17 and 18)**	590,076	597,989
Capital and total exposures			
20	**Tier 1 capital**	484,977	480,048
21	**Total Exposures (sum of lines 5, 11, 16 and 19)**	3,713,809	3,474,203
Leverage ratio			
22	**Basel III leverage ratio**	13.06%	13.82%

General qualitative information about credit risk

General qualitative information about credit risk – CRA

For the year 2024

(a) How the business model translates into the components of the Bank's credit risk profile

The Bank makes an assessment of the objective of a business model in which an asset is held at portfolio level because this best reflects the way the business is managed and information is provided to management. The information considered includes, amongst others, the stated policies and objectives for the portfolio and the operation of those policies in practice and how the performance of the portfolio is evaluated and reported to the Bank's management.

(b) Criteria and approach used for defining credit risk management policy and for setting credit risk limits

The Board of Directors (the "Board") has overall responsibility for the establishment and oversight of the Bank's risk management framework. The Board sets the Bank's risk appetite, including limiting concentrations of credit risk exposure to counterparties, industries and products. The management of the Bank has established the Risk Management Committee, Asset and Liability Management Committee ("ALCO"), Operational Risk Management Committee ("ORMC") and Credit Committee, which are authorized by the Board, to be responsible for developing and monitoring the Bank's risk management policies in their specified areas and recommending them to the Board.

The Bank has established the credit management policies and procedures that comply with the framework established by the parent bank and all of the standards, as determined by the governing regulatory bodies in Canada.

(c) Structure and organisation of the credit risk management and control function

The Board has delegated responsibility for the management of credit risk to the Credit Committee established by the management of the Bank. A separate Credit Risk Management Department, reporting to the Credit Committee and the Chief Risk Officer, is responsible for oversight of the Bank's credit risk, including:

- Formulating credit policies within the framework established by the parent bank and in consultation with the business units, covering collateral requirements, credit assessment, risk grading and reporting documentary and legal procedures and compliance with regulatory and statutory requirement.
- Establishing the authorization structure for the approval and renewal of credit facilities. Authorization limits are allocated to the Chief Executive Officer, the Chief Risk Officer and business unit Lending Officers. Larger facilities require approval by the Executive Committee of the Board, as appropriate.
- Reviewing and assessing credit risk. The Credit Risk Management Department assesses all credit exposures in excess of the authorization limits allocated to the business unit Lending Officers prior to facilities being committed to customers by the business unit concerned. Renewals and reviews of facilities are subject to the same review process.
- Limiting concentrations of exposure to counterparties, industries and products.

- Developing and maintaining the Bank's borrower gradings in order to categorize exposures according to the degree of risk of financial loss faced and to focus management on the attendant risks. The borrower grading system is used in determining where impairment provisions may be required against specific credit exposures.
- Reviewing compliance of business units with agreed exposure limits, including those for selected industries and product types.

(d) Relationships between the credit risk management, risk control, compliance and internal audit functions

Each business unit is required to implement the Bank's credit policies, with credit approval authorities delegated from the Board. Each business unit is responsible for the quality and performance of its credit portfolio and for monitoring and controlling all credit risks in its portfolios, including those subject to central approval. Regular audits of business units and the Credit Risk Management Department processes are undertaken by Internal Audit.

(e) Scope and main content of the reporting on credit risk exposure and on the credit risk management function to the executive management and to the board of directors

Senior management reports to the Board at least quarterly on material credit risk matters, including material credit transactions, compliance with limits, portfolio trends, impaired loans and credit loss provisioning levels. Provision for (reversal of) credit losses is reviewed by the Audit Committee quarterly. Regular reports are prepared by the Credit Risk Management Department and provided to the Credit Committee on the credit quality of local portfolios and appropriate corrective action is taken.

General qualitative information on operational risk framework

General qualitative information on operational risk framework –ORA

For the year 2024

(a) Policies, frameworks and guidelines for the management of operational risk

Operational risk at the Bank is defined based on the seven operational loss categories provided by the Basel Committee: internal fraud; external fraud; employment practices and workplace safety; clients, products and business practices, damage to physical assets, business disruption and system failures, and execution, delivery and process management.

The Bank has in place an effective Operational Risk Framework (‘the Framework’) and risk appetite for managing operational risk; key elements include: 1) communication/promotion of a positive/strong risk culture, 2) establishment of a clear risk governance structure, 3) risk taxonomy and risk identification, 4) risk assessment and measurement and 5) operational risk monitoring, and reporting processes.

Supporting the Framework, the Bank has a number of Board approved policies and Business Unit procedures in place including those related to operational resilience and operational risk management, the code of conduct, integrity and security, anti-money laundering, anti-terrorist financing, information security, third party and internal controls. Procedure manuals covering Front line Business Unit, Governance Units and Internal Audit Activities are in place and include a formal review and approval process.

(b) Structure and organisation of the operational risk management and control function

The structure and organization of the Bank’s operational risk (OR) management is based on the three lines of defense principle with the Board having ultimate oversight responsibility. Under the supervision of the Board, Senior Management is responsible for reviewing significant OR matters through the Operational Risk Management Committee. Given the pervasive nature of operational risk, every employee at the Bank is expected to play a role in managing operational risk.

Business Units, acting as the 1st line of defense (LOD), are responsible for the OR management within each of their respective business areas; Risk Management Department (“RMD”), Compliance and other functional departments, acting as the 2nd line of defense, are responsible for providing oversight/effective challenge, including the development of OR policies, measurement and monitoring/reporting. Internal audit department, acting as the 3rd line of defense, is responsible for independently reviewing and validating the implementation, appropriateness and effectiveness of OR and ORM.

(c) Operational risk measurement system

The Bank utilizes a number of qualitative and quantitative measurement tools/methodologies, supported by robust management information systems, in order to measure operational risk. Key quantitative measurement methodologies include: Operational Risk Capital Charge, using the Simplified Standardized Approach, and Operational Risk Appetite / Key Risk Indicators including those related to operational risk losses regulatory penalties, IT and cyber security, AML and compliance, customer complaint resolution, third party risk, human resources/employee turnover, training and employ misconduct. Key qualitative methodologies include business impact assessments and risk and control self-assessments.

Overseen by RMD, Risk and Control Self-Assessments (RCSA) are completed by every Business Unit on annual basis. The process involves each Business Unit identifying, for each applicable critical operation, key processes and related key risks, based on the operational risk taxonomy. Once identified, each Business Unit assesses if existing controls are sufficient/the residual risk is within limits/thresholds. RMD, along with other Governance Units, review the self-assessments to arrive at a final assessment.

If existing controls are assessed as insufficient, the Business Unit is responsible for developing remediation plans, as applicable. Action plans addressing significant residual risks, key control weaknesses, or significant breaches are given higher priority. RMD is responsible for monitoring progress.

(d) Scope and main context of the reporting framework on operational risk to executive management and to the board of directors

The Bank has in place a suite of reports, including those related to operational risk capital and operational risk appetite, which are regularly reviewed by the Board and Senior Management. These reports are a key mechanism in the continual enhancement of the Bank's operational readiness.

In support of the reporting processes, the Bank has a clear set of escalation procedures in place to ensure the appropriate actions, as needed, are implemented on a proactive basis. This includes having a tiered (i.e., early warning) risk appetite limit structure and an established culture of ongoing monitoring by all Departments.

(e) Risk mitigation and risk transfer used in the management of operational risk

There are a number of risk mitigation/risk transfer mechanisms available/used by the Bank in the management of operational risk. These include:

a) Mitigation by Operational Risk Policies – the Bank has established a comprehensive set of operational risk policies, including those related to operational resilience, integrity and security, third party risk and risk appetite.
b) Preventative and Detective Controls – the Bank has in place a wide ranging set of controls to mitigate operational risk.
c) Established Business Continuity Plans and Crisis Management Plans - Overseen by the Operational Risk Management Committee, the Bank, on a holistic/enterprise basis, has in place business continuity plans (BCP). BCPs enable the Bank to respond to a disruptive event on a timely and effective basis. The plans are updated on an annual basis and are subject to an annual test plan developed by RMD and the stakeholder departments.
d) The Bank has the option of using insurance to transfer risk.
e) As a very last resort, the strong capital position of the Bank allows the Bank to absorb any remaining exposure.