J.P. Morgan Bank Canada

Pillar 3 Disclosures

For the quarter ended April 30, 2026

J.P.Morgan

Table of contents

J.P. Morgan Bank Canada
Pillar 3 Disclosure
(in thousands of Canadian dollars)

General information

J.P. Morgan Bank Canada ("Bank") is a wholly-owned subsidiary of J.P. Morgan International Finance Limited of the United States and is licensed to operate as a bank in Canada with full banking powers under the Bank Act. The ultimate parent is JPMorgan Chase & Co. of the United States ("the Firm"). The address of the Bank's registered office is 66 Wellington Street West, Suite 4500, Toronto, Ontario M5K 1E7.

The Bank's main activity is the issuance of principal protected notes.

Capital management

The Bank manages and monitors its capital in accordance with the Office of Superintendent of Financial Institutions ("OSFI") guidelines, which are based on standards issued by the Bank for International Settlements. The Bank is segmented into Category II of the OSFI Small and Medium-Sized Deposit Taking Institutions Capital and Liquidity Requirements Guideline ("SMSB-CLR").

The Bank's regulatory capital consists of common equity tier 1 capital, which includes the more permanent components of capital and consists of shareholder's equity net of deferred tax assets. Regulatory ratios are calculated by dividing regulatory capital by risk-weighted assets ("RWA"). The RWA calculation is determined by OSFI-prescribed rules relating to on-and off-balance sheet exposures and includes minimum capital requirements for market and operational risk.

DIS20 - KM1: Key metrics on RWA

Quarter ended		April 30, 2026	January 31, 2026	October 31, 2025	July 31, 2025	April 30, 2025
	Available capital (amounts)					
1	Common Equity Tier 1 (CET1)	19,109	19,033	18,984	18,714	18,675
2	Tier 1	19,109	19,033	18,984	18,714	18,675
3	Total capital	19,109	19,033	18,984	18,714	18,675
	Risk-weighted assets (amounts)					
4	Total risk-weighted assets (RWA)	4,752	4,996	5,124	5,520	5,868
4a	Total risk-weighted assets (pre-floor)	4,752	4,996	5,124	5,520	5,868
	Risk-based capital ratios as a percentage of RWA					
5	CET1 ratio (%)	402.13	380.96	370.49	339.02	318.25
5a	CET1 ratio (%) (pre-floor ratio)	402.13	380.96	370.49	339.02	318.25
6	Tier 1 ratio (%)	402.13	380.96	370.49	339.02	318.25
6a	Tier 1 ratio (%) (pre-floor ratio)	402.13	380.96	370.49	339.02	318.25
7	Total capital ratio (%)	402.13	380.96	370.49	339.02	318.25
7a	Total capital ratio (%) (pre-floor ratio)	402.13	380.96	370.49	339.02	318.25
	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 (%)	-	-	-	-	-
10	Bank G-SIB and/or D-SIB additional requirements (%) **[Not applicable for SMSBs]**					
11	Total of bank CET1 specific buffer requirements (%) (row 8 + row 9 + row 10)	2.50	2.50	2.50	2.50	2.50
12	CET1 available after meeting the bank's minimum capital requirements (%)	399.63	378.46	367.99	336.52	315.75
	Basel III Leverage ratio					
13	Total Basel III leverage ratio exposure measure	19,783	19,655	20,626	22,164	21,849
14	Basel III leverage ratio (row 2 / row 13)	96.59%	96.84%	92.04%	84.43%	85.47%

(in thousands of Canadian dollars)

Modified CC1: Composition of regulatory capital

Quarter ended		April 30, 2026
	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	10,104
2	Retained earnings	9,023
3	Accumulated other comprehensive income (and other reserves)	(13)
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**	19,114
	Common Equity Tier 1 capital: regulatory adjustments	
28	**Total regulatory adjustments to Common Equity Tier 1**	(5)
29	**Common Equity Tier 1 capital (CET1)**	19,109
	Additional Tier 1 capital: instruments	
30	Directly issued qualifying Additional Tier 1 instruments plus related stock surplus	-
31	of which: classified as equity under applicable accounting standards	-
32	of which: classified as liabilities under applicable accounting standards	-
33	*Directly issued capital instruments subject to phase out from Additional Tier 1 (applicable only to Federal Credit Unions)*	-
34	Additional Tier 1 instruments (and CET1 instruments not included in row 5) issued by subsidiaries and held by third parties (amount allowed in group AT1)	-
35	*of which: instruments issued by subsidiaries subject to phase out (applicable only to Federal Credit Unions)*	-
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)**	19,109
	Tier 2 capital: instruments and provisions	
46	Directly issued qualifying Tier 2 instruments plus related stock surplus	-
47	*Directly issued capital instruments subject to phase out from Tier 2 (applicable only to Federal Credit Unions)*	-
48	Tier 2 instruments (and CET1 and AT1 instruments not included in rows 5 or 34) issued by subsidiaries and held by third parties (amount allowed in group Tier 2)	-
49	*of which: instruments issued by subsidiaries subject to phase out (applicable only to Federal Credit Unions)*	-
50	Collective allowances	-
51	**Tier 2 capital before regulatory adjustments**	-
	Tier 2 capital: regulatory adjustments	
57	**Total regulatory adjustments to Tier 2 capital**	-
58	**Tier 2 capital (T2)**	-
59	**Total capital (TC = T1 + T2)**	19,109
60	**Total risk-weighted assets**	4,752
	Capital ratios	
61	Common Equity Tier 1 (as a percentage of risk-weighted assets)	402.13%
62	Tier 1 (as a percentage of risk-weighted assets)	402.13%
63	Total capital (as a percentage of risk-weighted assets)	402.13%
	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%

Refer to OSFI's financial data for banks for additional information:
https://open.canada.ca/data/en/dataset/91ed76b4-a1a2-4f87-9c4c-59cd64f7a9de

Credit risk

DIS40 - CRA: General qualitative information about credit risk

Risk definition

Credit risk is the risk associated with the default or change in credit profile of a client, counterparty, or customer. JPMC is exposed to credit risk through its underwriting, lending, market-making, and hedging activities with and for clients and counterparties, as well as through its operating services activities and securities financing activities. The Firm is also exposed to credit risk through its investment securities portfolio and cash placed with banks.

Risk governance and policy framework

Credit Risk Management monitors, measures, and manages credit risk throughout the Firm and defines credit risk policies and procedures. The Firm's credit risk management governance includes the following activities:

- Maintaining a credit risk policy framework
- Monitoring and managing credit risk across all portfolio segments, including transaction and exposure approval
- Setting industry and geographic concentration limits, as appropriate, and establishing underwriting guidelines
- Assigning and monitoring credit authorities in connection with the approval of all credit exposure
- Managing criticized exposures and delinquent loans, and
- Estimating credit losses and ensuring appropriate credit risk-based capital management.

JPMC has developed policies and practices that are designed to preserve the independence and integrity of the approval and decision-making process to extend credit so that credit risks are assessed accurately, approved properly, and monitored regularly at both the transaction and portfolio levels. The firm-wide policy framework establishes credit approval authorities, concentration limits, risk-rating methodologies, portfolio review parameters and guidelines for management of distressed exposures.

Risk measurement

To measure credit risk the Firm employs several methodologies for estimating the likelihood of obligor or counterparty default. Methodologies for measuring credit risk vary depending on several factors, including type of asset, risk measurement parameters and risk management and collection processes. Counterparty risk relies upon multiple measures to capture, monitor, and control counterparty credit risk.

Risk monitoring

The policy framework establishes credit approval authorities, concentration limits, risk-rating methodologies, portfolio review parameters and guidelines for management of distressed exposures. In addition, certain models, assumptions, and inputs used in evaluating and monitoring credit risk are independently validated by groups that are separate from the lines of businesses (“LOB”).

Risk reporting

To enable monitoring of credit risk and effective decision-making, aggregate credit exposure, credit quality forecasts, concentration levels and risk profile changes are reported regularly to senior members of Credit Risk Management. Through the risk reporting and governance structure, credit risk trends and limit exceptions are provided regularly to, and discussed with, risk committees, senior management and the JPMC Board.

Structure and organization of the Credit Risk Management

JPMBC maintains a credit risk management framework, aligned with JPMC's standards. The Credit Risk Management function is led by the Chief Risk Officer ("CRO") for the Bank, who is responsible for independent oversight of credit risk across all business activities. The CRO and dedicated credit risk staff develop and implement credit risk policies, set risk limits, assign, and review internal risk ratings, monitor exposures and concentrations, and oversee the credit approval process. The Credit Risk Management function operates independently from the LOBs and reports directly to the Firm's CRO, who in turn reports to the Firm's senior management and the JPMC Board Risk Committee.

Relationships between Credit Risk Management, Risk Control, Compliance, and Internal Audit Functions

JPMBC's risk governance follows a "three lines of defense" model:

- First line: LOBs own and manage credit risk within approved policies and limits.
- Second line: The independent credit risk management function provides oversight and challenge to the first line and works closely with Risk Control and Compliance to ensure adherence to internal policies and regulatory requirements.
- Third line: Internal audit provides independent assurance on the effectiveness of credit risk management, controls, and governance.

These functions maintain regular communication and participate in relevant risk committees to ensure credit risk issues are identified, escalated, and addressed appropriately.

Credit valuation adjustment risk

DIS51 - CVAA: General qualitative disclosure requirements related to CVA

Basel III includes capital charges for counterparty default risk and credit valuation adjustments ("CVA"). CVA is a fair value adjustment to reflect counterparty credit risk in the valuation of over-the-counter derivatives. The Bank calculates CVA RWA using the reduced basic approach for CVA ("BA-CVA") which uses the Standardized Approach for Counterparty Credit Risk ("SACCR") exposure at default for each netting set.

DIS51 - CVA1: The reduced basic approach for CVA (BA-CVA)

April 30, 2026		Components	Capital requirements under BA-CVA
1	Aggregation of systematic components of CVA risk	2	
2	Aggregation of idiosyncratic components of CVA risk	6	
3	**Total**		-

Operational risk

DIS60 - ORA: General qualitative information on a bank's operational risk framework

Risk definition

Operational risk is the risk of an adverse outcome resulting from inadequate or failed internal processes or systems, human factors, or external events impacting the Firm's processes or systems.

Operational risk is inherent in the Firm's activities and can manifest itself in various ways, including fraudulent acts, business disruptions (including those caused by extraordinary events beyond the Firm's control), cyber-attacks, technology process failure, inappropriate employee behavior, failure to comply with applicable laws, rules and regulations or failure of vendors or other third-party providers to perform in accordance with their agreements. The

Firm attempts to manage operational risk at appropriate levels considering the Firm's financial position, the characteristics of its businesses, and the markets and regulatory environments in which it operates.

Compliance, Conduct and Operational Risk ("CCOR") Management Framework

The CCOR Management Framework is designed to enable the Firm to govern, identify, measure, monitor and test, manage and report on the Firm's operational risk compliance, conduct, and operational risks.

The Firm's Global Chief Compliance Officer ("CCO") and Firmwide Risk Executive ("FRE") for Operational Risk Management ("ORM") and Qualitative Risk Appetite, a direct report to the Firm's CRO, is responsible for establishing and defining the CCOR Management Framework and establishing minimum standards for its execution. The LOB, Control Functions ("CF") and Regional CCOR Officers report to the Global CCO and FRE for ORM and Qualitative Risk Appetite and are independent of the respective LOBs or CFs they oversee. The CCOR Management Framework is included in the Risk Governance and Oversight Policy that is reviewed and approved by the JPMC Board Risk Committee periodically.

The components of the CCOR Management Framework are:

Govern

The CCOR organization establishes policies and standards which set forth the requirements for the LOBs and CFs regarding the management and oversight of compliance, conduct, and operational risks inherent within the Firm's activities.

Key documents applicable to the management of compliance risk will include:

- CCOR Management Governance Policy – Firmwide
- CCOR Management Standard – Firmwide
- Compliance and Operational Risk Evaluation ("CORE") Standard – Firmwide; and
- JPMC Code of Conduct.

The LOBs and CFs execute the CCOR management framework and manage the compliance, conduct, and operational risks that arise from their activities. Control Managers, who are members of the LOBs and CFs and part of the Control Management Organization, partner with LOB and CF executives and first line of defense process owners in control design, control evaluation and issue management of operational risks. They are responsible for the day-to-day execution of the CCOR Framework and will determine where targeted remediation efforts may be required based on the effectiveness of their control environments. LOBs and CFs regularly monitor their risks and evaluate that established controls are functioning as expected (control performance) and are effective in managing risks (control design).

The CCOR organization raises issues for the LOBs and CFs to remediate through action plans on an as-needed basis to mitigate and reduce compliance, conduct and operational risks. These are captured in the CORE system of record. The status of these issues is reported through the appropriate LOB or CF Control Committees. CCOR also provides challenge to the issues identified and action plans developed by the LOBs and CFs and provides objection or non-objection for certain items as outlined in the Operational Risk Issue Management Standard.

Identify

CCOR maintains and manages risk taxonomies which are used to organize and categorize Firm's compliance and operational risks, controls and processes and are leveraged to support identification, measurement, analysis, reporting and assessment activities within CCOR organization and across LOBs and CFs in a consistent way.

Measure

The Firm assesses its compliance, conduct and operational risks as well as the effectiveness of its controls within CORE, the Firm's structured risk and control self-assessment process. LOBs and CFs own and manage the

compliance, conduct and operational risks inherent within the processes they execute and therefore are responsible for the identification, assessment and ongoing management of those risks, and the design, execution, and evaluation of associated controls.

The CCOR organization sets the CORE Standards and the LOB and CF Compliance Officers and Operational Risk Officers provide oversight and challenge of the risks identified and of the assessment results, and then utilize these results to drive the CCOR organization's activities and priorities on a risk-based approach. The CCOR organization may also perform independent assessments of significant operational risk events and/or areas of concentrated or emerging risk.

Monitoring & Testing

The results of compliance, conduct and operational risk measurement and identification activities undertaken by the CCOR organization and LOBs and CFs are leveraged as one of the key criteria determining the CCOR organization independent assurance activities on a risk-based approach to evaluate LOBs and CFs compliance with laws, rules and regulations, as well as internal policies, standards and procedures. Through the assurance activities, the CCOR organization independently identifies areas of heightened compliance, conduct and operational risks and tests the effectiveness of controls within the LOBs and CFs.

Report

Escalation of risks is a fundamental expectation for employees at JPMC. Risks identified by the LOBs and CFs and the CCOR organization, as part of regular day to day activities or management routines, may be escalated to the appropriate LOB and CF Control Committees, then to the Firmwide Control Committee, which may, in turn, escalate to the Firmwide Risk Committee, and JPMC Board Risk Committee as appropriate and necessary.

The CCOR organization produces various firmwide Board-level and senior management reports to facilitate firmwide compliance, conduct and operational risk management activities. These reports are an important means of escalating risk events and CCOR tracked metrics to the Firm's risk governing bodies. These may be on a business as usual or non-business as usual basis. The CCOR organization also participates in Control Committee reporting.

Compliance, conduct and operational risk events may result in financial losses, litigation, and regulatory fines as well as other damages to the Firm.

Internal operational risk events are those that occur within the Firm or vendors of the Firm. Data on internal risk events is leveraged for a variety of reporting uses, including the development of projected losses in the Stress Loss Projection framework as well as reporting to senior management.

External operational risk events are those incurred outside the Firm. Data on external risk events provides valuable insight when managing and measuring compliance, conduct and operational risk in the context of our peers and the general industry.

Operational risk can manifest itself in various ways. Business and technology resiliency and cybersecurity risks are managed at the firmwide level and assessed as part of the CCOR Framework. Below provides the firmwide view of these risks.

Firmwide resiliency risk

Disruptions of the Firm's business and operations can occur due to forces beyond the Firm's control such as the spread of infectious diseases or pandemics, severe weather, natural disasters, the effects of climate change, power or telecommunications loss, failure of a third party to provide expected services, cyberattacks, civil or political unrest or terrorism. The Firm's resiliency framework is intended to enable the Firm to prepare for and adapt to changing conditions and withstand and recover from, and address adverse effects on its operations caused by, disruptions that may impact critical business functions and supporting assets, including its staff, technology, data and facilities, as well as those of third-party service providers. The framework includes governance, awareness training, planning and

testing of recovery strategies, as well as strategic and tactical initiatives to identify, assess, and manage resiliency risks. The framework operates in accordance with the Firm's overall approach to ORM, including alignment with technology, cybersecurity, data, physical security, crisis management, real estate and outsourcing programs.

Cybersecurity risk

Cybersecurity risk is the risk of the Firm's exposure to harm or loss resulting from misuse or abuse of technology or the unauthorized disclosure of data.

Cybersecurity risk is an important and continuously evolving focus for the Firm. Significant resources are devoted to protecting and enhancing the security of computer systems, software, networks, storage devices, and other technology. The Firm's security efforts are designed to protect against, among other things, cybersecurity attacks that can result in unauthorized access to confidential information, the destruction of data, disruptions to or degradations of service, the sabotaging of systems or other damage.

The Firm has experienced, and expects that it will continue to experience, a higher volume and complexity of cyber-attacks against the backdrop of heightened geopolitical tensions. The Firm has implemented measures and controls reasonably designed to address this evolving environment, including enhanced threat monitoring. In addition, the Firm continues to review and enhance its capabilities to address associated risks, such as those relating to the management of administrative access to systems.

Third parties with which the Firm does business or that facilitate the Firm's business activities (e.g., vendors, supply chain, exchanges, clearing houses, central depositories, and financial intermediaries) or that the Firm has acquired are also sources of cybersecurity risk to the Firm. Third party incidents such as system breakdowns or failures, misconduct by the employees of such parties, or cyber-attacks, including ransomware and supply-chain compromises, could have a material adverse effect on the Firm, including in circumstances in which an affected third party is unable to deliver a product or service to the Firm or where the incident delivers compromised software to the Firm or results in lost or compromised information of the Firm or its clients or customers.

Clients and customers are also sources of cybersecurity risk to the Firm and its information assets, particularly when their activities and systems are beyond the Firm's own security and control systems.

The Firm engages in periodic discussions with its clients, customers and other external parties concerning cybersecurity risks and opportunities including opportunities to improve cybersecurity.

Risks from cybersecurity threats, including any previous cybersecurity events, have not materially affected the Firm or its business strategy, results of operations or financial condition. Notwithstanding the comprehensive approach that the Firm takes to address cybersecurity risk, the Firm may not be successful in preventing or mitigating a future cybersecurity incident that could have a material adverse effect on the Firm or its business strategy, results of operations or financial condition.

Organization and management

The Global Chief Information Security Officer ("CISO") reports to the Global Chief Information Officer ("CIO") and is a member of key cybersecurity governance forums. The CISO leads the Global Cybersecurity and Technology Controls organization, which is responsible for identifying technology and cybersecurity risks and for implementing and maintaining controls to manage cybersecurity threats. The CISO and the members of senior management within Global Technology and the Cybersecurity and Technology Controls organizations all have relevant expertise and experience in cybersecurity and information technology risk management, including relevant experience at the Firm, at other financial services companies or in other highly regulated industries.

The CISO is responsible for the Firm's Information Security Program, which is designed to prevent, detect, and respond to cyber-attacks in order to help safeguard the confidentiality, integrity and availability of the Firm's infrastructure, resources and information. The program includes managing the Firm's global cybersecurity operations centers, providing training, conducting cybersecurity event simulation exercises, implementing the

Firm's policies and standards relating to technology risk and cybersecurity management, and enhancing, as needed, the Firm's cybersecurity capabilities.

The Firm's Information Security Program includes the following functions:

Cyber Operations, which is responsible for implementing and maintaining controls designed to detect and defend the Firm against cyber-attacks and includes a dedicated function for incident response and ongoing monitoring for cybersecurity threats and vulnerabilities, including those among the Firm's third-party suppliers.

Technology Governance, Risk & Controls, which is responsible for operationalizing technology risk and control frameworks, analyzing regulatory developments that may impact the Firm, and developing control catalogues and assessments of controls, as well as overseeing governance and reporting of technology and cybersecurity risk.

Security Awareness, which provides awareness and training that reinforces information risk and security management practices and compliance with the Firm's policies, standards and practices. The training is mandatory for all employees globally on a periodic basis, and it is supplemented by Firmwide testing initiatives, including periodic phishing tests. The Firm also provides specialized security training to employees in specific roles, such as application developers. The Firm's Global Privacy Program requires all employees to take periodic training on data privacy that focuses on confidentiality and security, as well as responding to unauthorized access to or use of information.

Technology Resiliency, which establishes control requirements for planning and testing the prioritized recovery of technology services in the event of degradation or outage, including incident response planning, data backup and retention, and recovery readiness in support of the Firmwide Business Resiliency Program and operational risk management practices.

The Firm has a cybersecurity incident response plan designed to enable the Firm to respond to attempted cybersecurity incidents, coordinate as appropriate with law enforcement and other government agencies, notify clients and customers, as applicable, and recover from such incidents. In addition, the Firm actively partners with appropriate government and law enforcement agencies and peer industry forums, participating in discussions and simulations to assist in understanding the full spectrum of cybersecurity risks and in enhancing defenses and improving resiliency in the Firm's operating environment.

Insurance

One of the ways in which operational risk may be mitigated is through insurance maintained by the Firm. The Firm purchases insurance from commercial insurers and maintains a wholly owned captive insurer, Park Assurance Company. Insurance may also be required by third parties with whom the Firm does business.

Governance and oversight

The governance structure for the Global Cybersecurity and Technology Controls organization is designed to appropriately identify, escalate, and mitigate cybersecurity risks. Cybersecurity risk management and its governance and oversight are integrated into the Firm's operational risk management framework, including through the escalation of key risk and control issues to management and the development of risk mitigation plans for heightened risk and control issues. Independent Risk Management ("IRM") independently assesses and challenges the activities and risk management practices of the Global Cybersecurity and Technology Controls organization related to the identification, assessment, measurement, and mitigation of cybersecurity risk. As needed, the Firm engages third-party assessors or auditing firms with industry-recognized expertise on cybersecurity matters to review specific aspects of the Firm's cybersecurity risk management framework, processes, and controls.

The governance and oversight for cybersecurity risk management includes governance forums that inform management of key areas of concern regarding the prevention, detection, mitigation and remediation of cybersecurity risks.

The Cybersecurity and Technology Controls Operating Committee ("CTOC") is the principal management committee that oversees the Firm's assessment and management of cybersecurity risk including oversight of the implementation and maintenance of appropriate controls in support of the Firm's Information Security Program. The membership of the CTOC includes senior representatives from the Global Cybersecurity and Technology Controls organization and relevant CFs, including IRM and Internal Audit.

The CTOC escalates key operational risk and control issues, as appropriate, to the Global Technology Operating Committee ("GTOC") or its business control committee or to the appropriate LOB and Corporate Control Committees. The GTOC is responsible for the governance of the Firmwide Global Technology organization, including oversight of Firmwide technology strategies, the delivery of technology and technology operations, the effective use of information technology resources, and monitoring and resolving key operational risk and control matters arising in the Global Technology organization.

As part of its oversight of management's implementation and maintenance of the Firm's risk management framework, the Firm's Board of Directors receives periodic updates from the CIO, the CISO and senior members of the CTOC concerning cybersecurity matters. These updates generally include information regarding cybersecurity and technology developments, the Firm's Information Security Program and recommended changes to that program, cybersecurity policies and practices, and ongoing initiatives to improve information security, as well as any significant cybersecurity incidents and the Firm's efforts to address those incidents. The Firm's Audit Committee and Board Risk Committee assist the Board in this oversight.

Risk appetite

Risk appetite is a high-level statement of the Firm's appetite for risk and reflects the "tone at the top" by the Firm's senior management and the Board of Directors.

The FRE of Qualitative Risk Appetite is responsible for developing the Firmwide Qualitative Risk Appetite framework, inclusive of the Qualitative Risk Appetite statement, which includes the following risk areas: Compliance, Conduct, Reputation and Operational. The framework outlines a qualitative evaluation that is supported by quantitative measures (metrics).

LOBs and CFs are owners of the risks and must identify, manage, and control these risks to remain within appetite.

The CCOR organization, as the second line of defense, provide challenge of the firmwide assessment of qualitative risk appetite for each area and report the results to senior management and the Board. Each risk is managed through the qualitative risk appetite framework as described in the Firm's Qualitative Risk Appetite Policy. The CCOR organization is responsible for the setting of the framework and the management/oversight of the process each quarter.

Risk governance and policy framework

JPMBC follows the Firm's CCOR Framework, adjusting to the local regulatory requirements whenever different than the Firm's procedures.

Legal entity measurement

In addition to losses associated with operational risk events, another measure of operational risk is the minimum capital requirement calculated using the Simplified Standardized Approach. It considers a beta factor of 15% over the 3-year average annual adjusted gross income i.e. the sum of (a) the lesser of (i) the absolute value of net interest income, and (ii) 2.25% of interest earning assets; (b) the absolute value of fee and commission income; (c) the absolute value of other income; and (d) the absolute value of net profit/loss of trading book.

(in thousands of Canadian dollars)

Leverage ratio

DIS80 - LR2: Leverage ratio common disclosure template

Quarter ended		April 30, 2026	January 31, 2026
On-balance sheet exposures			
1	On-balance sheet items (excluding derivatives, SFTs and grandfathered securitization exposures but including collateral)	19,785	19,651
2	Gross-up for derivatives collateral provided where deducted from balance sheet assets pursuant to the operative accounting framework (IFRS)	-	-
3	(Deductions of receivable assets for cash variation margin provided in derivatives transactions)	-	-
4	(Asset amounts deducted in determining Tier 1 capital)	(5)	(5)
5	**Total on-balance sheet exposures (excluding derivatives and SFTs) (sum of lines 1 to 4)**	19,780	19,646
Derivative exposures			
6	Replacement cost associated with all derivative transactions	-	-
7	Add-on amounts for potential future exposure associated with all derivative transactions	3	9
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)**	3	9
Securities financing transaction exposures			
12	Gross SFT assets recognised 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	-	-
18	(Adjustments for conversion to credit equivalent amounts)	-	-
19	**Off-balance sheet items (sum of lines 17 and 18)**	-	-
Capital and total exposures			
20	**Tier 1 capital**	19,109	19,033
21	**Total Exposures (sum of lines 5, 11, 16 and 19)**	19,783	19,655
Leverage ratio			
22	**Basel III leverage ratio**	96.59%	96.84%