Canadian Web3 Council

October 22, 2024

Office of the Superintendent of Financial Institutions
255 Albert Street 12th Floor
Ottawa, Ontario K1A 0H2

VIA EMAIL: Pillar3-Pilier3@osfi-bsif.gc.ca

RE: Submission to OSFI Consultation on Public Disclosure of Crypto-asset Exposures

The Canadian Web3 Council (CW3) is pleased to respond to the above consultation by the Office of the Superintendent of Financial Institutions (OSFI).

CW3 is a non-profit trade association founded by industry leaders to work constructively with policymakers and establish Canada as a leader in Web3 technology[1]. CW3 represents organizations that develop Web3 technologies across the globe and are committed to responsibly building and innovating in Canada. Our membership is diverse, ranging from hackathon organizers to investors and providers of financial products, trading platforms, and open-source blockchain projects.

Introduction

First, it is essential to recognize the limitations in the implementation of the current Pillar 3 disclosures. Challenging areas for both financial institutions (FIs) and regulators largely include disclosures around operational risk management. FIs disclose risk management practices that sound good on paper. Yet there can be a disconnect between disclosure and the decisions made with respect to the actual underlying risks when organizations fail to execute on either key controls or when the failures are systematic. **Recent examples[2] of operational failures involving activities undertaken by regulated traditional financial institutions give reasons to pause and reflect on Pillar 3 disclosures for banking activities and financial services more generally, and not simply those involving crypto assets. Market discipline requires management and regulators to have an appropriate response to operational risk. Failure to do so can turn operational risk into prudential risk.**

Our comments address consultation questions #1 and #2 through the lens of fiat-backed stablecoins, the involvement of fintechs under an open banking framework, and disclosures

[1] At its core, web3 technology aims to enable direct interactions between users without relying on intermediaries. It emphasizes the use of decentralized applications (dApps) that run on blockchain networks, where data and processes are distributed across a network of nodes, making them resistant to censorship, manipulation, and single points of failure. Overall, web3 technology represents a paradigm shift towards a more decentralized, open, and user-centric internet, empowering individuals and communities with greater control over their digital lives.

[2] Specifically banking as a service involving Synapse and TD Bank's AML compliance failures

around operational risk in general. Against the backdrop of recent failures in operational risk management involving banks, we ask whether the Pillar 3 disclosures will achieve their intended policy goals as described below.

- *To Protect* stakeholders[3] by ensuring appropriate information is available **for the public** to understand the *financial condition* of Canadian Federally Regulated Financial Institutions ("FRFIs") and federally regulated small and medium-sized deposit-taking institutions "SMSBs" *and the risks* to which they are exposed.

- Whether disclosure is an effective tool for better decision-making and market discipline by the financial institution.

General comments

Our comments focus on Pillar 3 disclosures around operational risk management involving crypto assets, third party relationships, and operational risk more generally. We highlight the following items for consideration:

1. *Application of materiality to on-balance sheet items.* When applying materiality, FIs should assess materiality by looking at on-balance sheet assets (e.g. tokenized crypto assets like investment funds) separately from on-balance sheet liabilities (e.g. tokenized deposits) because the nature of the risks is different. Canadians should understand that a deposit token (issued under fractional reserve banking) has a different risk profile from a Group 1b fiat-backed stablecoin ("FBSC") that is fully backed by high quality and liquid assets, held for the benefit of FBSC users.

   It is essential to recognize that for assets, there is the risk of an overstatement. For liabilities, the risk is a potential understatement. This nuanced difference is essential when applying judgment and decisions for making meaningful disclosures.

   With respect to the usefulness of disclosing aggregate group 2a and 2b crypto assets whether using daily average or period end values. Both are important. For any fiat-backed stablecoins[4] ("FBSCs"), the amount of FBSCs issued and outstanding using period end values is a liability which should be fully reserved by off-balance sheet assets comprising high quality liquid assets using period end values, and this condition must be true at all times. The crypto ecosystem refers to this as proof of reserves. For Pillar 3 reporting, an FBSC issuer should also disclose whether the period end value of the assets backing the FBSC was at least equal to the issued amount of FBSC at all times, and the length of time that an FBSC depegged, where applicable.

[3] which include depositors, policyholders, and creditors

[4] This condition applies to all FBSCs whether they fall under groups 1b, 2a and 2b

We ask you to consider drawing a distinction between crypto assets that are assets from those that are liabilities. We believe the materiality thresholds should also be applied to the absolute value of crypto asset exposures and not just the aggregate value of the exposures.

2. *Consider applying materiality to off-balance sheet risks.* Not all current or future financial services involving crypto assets will necessarily result in an on-balance sheet exposure (e.g., FBSC reserve assets, custody, certain third party partner arrangements under open banking, policy gaps etc). Failure to address operational risk can translate into material financial risk and/or going concern risk[5] for items i) that are not on balance sheet or, ii) that are key internal controls failures over an extended period of time. This has been demonstrated by recent operational risk failures involving traditional FIs and/or their fintech partners.

   The following instances require a more nuanced view of materiality and risk mitigation:

   a. Risks that involve non-financial off-balance sheet items, i.e., assets under custody, which can include digital assets. Whereas custody of off-chain assets, i.e., real world assets, require custodians to maintain records of what they hold for traditional finance entities, digital asset custody involves handling of the private keys to access digital assets. Differences in the nature of the service require a different approach to managing operational risk. Digital asset custodians can mitigate such risks by providing, for example, ongoing proof of reserve attestations together with SOC II type II reports and information security reviews. Disclosure should address these important matters.

   b. Systematic failures, i.e., failures that involve large parts of any organization (including their fintech partners), particularly when those who act in a control or oversight capacity fail to execute in a systematic way[6] (e.g., recent AML failures). For Pillar 3 disclosures, the lack of a bright line test for operational risks presents challenges for management, their boards and also for regulators as the failures may include a failure to respond with appropriate measures. Where regulators identify significant regulatory concerns, they need to be empowered to disclose concerns that may be in the public interest, and also be equipped with the appropriate tools to respond. Equally challenging is the delicate balance between maintaining the safety and soundness of an FI or the financial system and the public's right to know. All of these matters require careful consideration and exercise of judgment to disclose or not.

[5] Recent examples of operational risk failures include, penalties and fines levied under AML failures involving several Canadian D-SIBs. In the U.K., the shortfall in client funds arising from "for benefit of client" accounts and the insolvency of Synapse (a fintech under the banking as a service model)

[6] These functions may involve a large cross section of departments including operations, finance, internal audit, human resources,governance and oversight committees etc.

c. Many FIs describe using a “risk based approach” but provide little context to the public. One would expect FIs to report residual risks that exceed the entity’s risk appetite. FIs do not publicly disclose their risk tolerance leaving affected stakeholders (especially bank customers, including those who have been de-risked) with the challenging task of deciphering any disclosures to determine the impact of disclosed risk and whether there are undisclosed material risks. Losses associated with operational risk are typically recorded when it occurs. The public receives no disclosures of impending regulatory actions. Consequently, any resulting fines/penalties are perceived as a cost of doing business in consumers’ eyes and each occurrence chips away at confidence in the regulation of financial institutions.

3. *Failures in internal controls.* Internal control failures are examples of operational risk. e.g. the inability to track customer deposit account balances and funds flow can give rise to prudential risk under banking as a service model provided to fintech intermediaries, e.g. Synapse. Evidence of such risks are identified by reviewing account reconciliations, and the integrity of this process is dependent upon data quality, validating reconciling items and controls around segregation of duties. FIs may also need to consider indirect information (e.g. customer complaints either directly or through channel partners). FIs need to consider the totality of these internal control failures and apply judgment in determining not only whether and what to disclose, but also how to communicate such matters in a way that the information is understood by stakeholders.

   The inability of an FI to determine the balance of customer funds held and/or where they’re held presents a significant risk to consumers. This situation can arise when an FI has insufficient information to make a proper risk assessment or the reconciliations are not performed with sufficient frequency (i.e., daily). Moreover, the risk profile is dependent upon the account type, the nature of the commercial arrangements between fintech and FI, the complexity of funds flow particularly amongst affiliated parties, and the types of services being accessed and how. Performing frequent and proper reconciliation of accounts designated as trust accounts, or in the case of third party partners, for the benefit of client accounts are examples of such controls. These comments apply to traditional financial services as well as crypto asset services. It’s essential for an organization (and a regulator) to assess whether that failure can present a prudential risk or place consumers at risk.

4. *Material compliance failures* raise questions around an organization’s operational integrity and governance (including monitoring of third party service providers). A failure to remediate compliance failures is a risk that may require disclosure. Not all compliance missteps result in a fine. Some may give rise to a regulatory action. Under the present framework, the necessary Pillar 3 disclosures may not be made until the investigations are well underway, or a fine/penalty or regulatory action/sanctions results. In such situations,

policymakers should assess the disclosure obligations of regulators upon whom the Canadian public relies. We acknowledge that current laws may prevent regulators from naming entities that are under investigation for significant compliance deficiencies and these situations require careful consideration so as not to precipitate a crisis in confidence[7].

5. *Regulatory clarity around supervision.* We believe that fiat-backed stablecoins ("FBSC") are a digital money equivalent. There is currently no legislative framework for the use and issuance of FBSC in Canada. As a result, the Canadian Securities Authorities have stepped in to fill the void. The current lack of clarity between the intersections between prudential, securities and payments require attention. Processes that fall under different regulatory agencies such that no one agency has a 360-degree view of the controls can be more susceptible to regulatory failure. We believe that supervision and regulation of the use and issuance of FBSCs is better served under the purview of a federal agency given its function[8].

Recommendations

We believe that meaningful and fulsome disclosures can dispel common myths associated with crypto assets and use of innovative technologies. Providing the Canadian public with information to differentiate between the risk profiles of various tokenized products will become more important as banks compete with fintechs in making tokenized offerings, e.g., tokenized deposit tokens versus fiat-backed stablecoins. At the same time, we need to collectively find ways to improve the market disciplines around operational risk management and disclosures for both incumbents and fintechs.

To help Canadians better understand such risks and risk mitigation efforts, implementing measures to help Canadians improve their digital and financial literacy should also be a priority and can be addressed through public/private initiatives. Moreover, policymakers and regulators could benefit from more relevant data to drive policy decisions.

For these reasons, we recommend establishing a working group to address operational risk management (and data requirements) including third party liability and obligations. This working group would include representatives from affected regulatory agencies, and fintech representatives from crypto asset and banking sectors with a mandate to develop a fit for purpose risk management framework for the use and issuance of fiat-backed stablecoins/crypto assets and establishing third party partner relationships in traditional financial sectors.

[7] For example, See Statement from Superintendent of Financial Institutions re Toronto Dominion Bank Link Here

[8] For example, CW3 believes the use of FBSCs for payments should be regulated under the Retail Payment and Activities Act.