Office of the Superintendent of Financial Institutions Canada

Bureau du surintendant des institutions financières Canada

Capital Division Guidance / Rule-Making

February 2020
Internal Audit Report
Assurance Engagement

OSFI BSIF

Canada

Table of Contents

Glossary and Abbreviations

BCBS	Basel Committee on Banking Supervision
CED	Communications Engagement Division
CD	Capital Division
FRFIs	Federally Regulated Financial Institutions
GRC	Guideline Review Committee
IAIS	International Association of Insurance Supervision
MD	Managing Director
OSFI	Office of the Superintendent of Financial Institutions Canada
SME	Subject Matter Expert
TBS	Treasury Board Secretariat
TLS	Transport Layer Security

1. Background

1.1 Context

The Capital Division (CD) under the Regulation Sector is responsible for setting rules and related prudential standards for capital that Federally Regulated Financial Institutions (FRFIs) are required to hold. Capital rules and related standards and guidelines are foundational to the way the Office of the Superintendent of Financial Institutions Canada (OSFI) meets its mandate of regulating and supervising FRFI.

CD, headed by a Senior Director, is organized by Banking (Deposit Taking Institutions) and Insurance (Life Insurance, and Property and Casualty Insurance) under Managing Directors (MD). The Division also includes a Senior Advisor at the MD level.

With respect to guidance and rule making, CD supports OSFI's mandate by undertaking the following main objectives and related activities:

Rule Making ensures that:

- OSFI's capital rules and related prudential standards and guidelines are timely, clear and relevant, appropriately reflect industry and market practices, meet or exceed international minimums and are developed using an appropriate consultation process;
- An appropriate balance exists in rules between safety and soundness while taking into account the need to have a competitive environment in which FRFIs can succeed; and
- It contributes to the development of international regulations, standards, and rule making through its participation in international prudential regulation for such entities as the BCBS (Basel Committee on Banking Supervision) and the IAIS (International Association of Insurance Supervision).

CD has in place a rule making Framework document titled "Capital Division Rule Making Framework" (dated November 2010) (herein "the Framework") for use in the development of regulatory guidance. As described in the Framework, OSFI's rule making process consists of the following five-phase "*life cycle*" approach:

1) Initial analysis & policy
2) Approval to proceed
3) Guidance (rule development)
4) Consultation with Industry
5) Distribution (publishing), used for maintaining capital instrument rule guidance

The last Internal Audit completed in CD was the Capital Division Rule Making audit in July 2012.

1.2 Objective

The objective of the engagement was to provide reasonable assurance that:

- The Framework is adequate in supporting the rule making process, and aligned with recently established Government of Canada's policy instruments, as applicable; and
- The rule making process, documents and related aids/tools in place are functioning as intended and comply with the Framework.

Background, Continued

1.3 Statement of Conformance

The audit was conducted in conformance with the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing, consistent with the TBS (Treasury Board Secretariat) Policy on Internal Audit and the Internal Auditing Standards of the Government of Canada, as supported by the results of the Quality Assurance and Improvement Program.

1.4 Scope

The audit covered rule making activities for *Deposit Taking Institutions, Life Insurance, and Property and Casualty Insurance*. The areas of focus and scope of the engagement included:

- Reviewing the Framework in place to assess if the design elements are appropriate, and support the effective management of guidance development;
- Reviewing OSFI's current rule making guidance relating to Capital Adequacy Requirements and Sound Business & Financial Practices that were issued in 2018 and 2019, to ensure compliance with the Framework; and
- Reviewing aids/tools in place to ensure they are functioning as intended.

1.5 Procedures Performed

The audit involved three methods of examinations:

1. Review and examination of relevant aids/tools, processes, and the Framework in place;
2. Walkthroughs of various processes and procedures and a detailed review of a representative sample of selected guidance completed during fiscal April 2018 – March 31, 2019; and
3. Discussions with key CD staff, as appropriate.

2. Results of the Engagement

Overall, we observed that there exists a robust risk dashboard for managing guidance priorities of the division, established rule-making Framework and ongoing involvement of key staff with the international regulatory committees/conferences for staying abreast of regulatory environment and contributing to its development. While the Framework meets the rule making lifecycle principles of TBS policy instruments, enhancements as noted in the report are identified, along with opportunities for streamlining corresponding aids/tools.

Based on our discussions, CD analysts appear to know their files and perform their work based on their experience and knowledge; however, it was observed that analysts may not be as familiar with the Framework as CD management.

Additional observations and considerations pertaining to the following areas are contained in this report.

- Guidance documents and mechanisms should be updated and streamlined
- Formal approval authorities are not adequately explained
- IT security over email transmission require awareness
- Continuous improvement and quality control practices lack commitment
- Issues log is not managed, as designed in a coordinated/centralized manner

3. Management Response

3.1 Overview

This report has been reviewed by the Senior Director, Capital Division, and the Assistant Superintendent, Regulation Sector, who acknowledge its observations and recommendations. The report has also been reviewed by OSFI's Executive Committee.

3.2 Responses / Comments

The Capital Division wishes to express its many thanks to the audit team for the professional, and transparent way in which they conducted their audit. We agree with the recommendations of the audit team and will implement them by December 31, 2020.

In summary, we welcome the observations made by internal audit during this process. We believe that the updating of the 2010 Capital Division Framework will satisfy the majority of the observations identified. In addition, there are benefits that will extend beyond the Capital Division to be applicable to other areas within the Regulation Sector.

In the Capital Division the control of process and procedures is overseen by the management teams. The analysts are accountable for knowing the system and stages of policy development, while the responsibility for the adherence to the Framework lies with management. The inconsistent understanding and outdated sections of the Framework would explain why the breadth of responses from the analysts on the use of the Framework were received. The analysts rely on the checklists and playbooks more than the Framework. Part of our plans going forward will be update and consolidate the development tools to be used by all Capital Division staff.

The Capital Division also agrees with the observations and comments made that the referenced updates and consolidation will also benefit with the onboarding of new staff within the Division.

4. Observations and Recommendations

Observation #1: *Guidance documents and mechanisms should be updated and streamlined*

(Medium Priority)

The Framework

Recently issued TBS "Policy on Regulatory Development" (TBS Policy), 2018, expects federal regulators to comply with the Cabinet Directive on Regulation (the Directive) as it relates to the process of developing regulations. Additionally, TBS "Guidelines for Effective Regulatory Consultations" (TBS Consultations Guidelines) provides tools to support effective consultations throughout the regulatory life cycle. Although CD does not develop regulations, the underlying principles and expectations identified in TBS Policy and the TBS Consultations Guidelines are considered benchmark practices when developing guidance and largely applicable to the development of regulatory guidance within a federal organization such as OSFI.

Based on our review we noted that, while the Framework fares well against the TBS policy instruments, aspects of the Framework makes reference to dated information (i.e. Risk Tolerance Framework, Electronic Document Management System (EDMS), etc.) and require updating: 1) alignment with TBS regulation development principles and the TBS Consultations Guidelines, 2) current CD structure and practices, and 3) clarification of expectations and responsibilities.

TBS Policy guidance outlines the final phase of the life-cycle as the review and assessment of the results of regulation/[guidance]. As part of CD's practice this is understood as being embedded as part of the cyclical nature of CD's current practices with the review of all guidance on an annual basis against various inputs (i.e. industry inquiries, international regulations, etc.). However, the Framework does not outline the expectations surrounding the process for ensuring guidance continue to be appropriate, effective and achieve CD's intended objectives, along with outlining associated roles and responsibilities. Similarly, Section 4.2 of the TBS Consultations Guidelines discusses the need to establish a consultation plan in order to achieve the goals and objectives of the proposed regulation/[guidance] and facilitate a smooth consultative process. The Framework is silent on the consultation process development.

Not having an updated Framework in place, could create challenges for existing and newly onboarded CD staff that rely on the Framework for guidance development. This would increase the risk that OSFI's regulatory guidance development is not aligned with CD management expectations or current accepted practices.

Governance Committees

As part of the governance mechanisms in place, OSFI has a Guideline Review Committee (GRC), chaired by Regulatory Affairs Division (RAD), of which Capital Division is a member. GRC prepares and monitors a holistic view of OSFI's guidance priorities, along with ensuring consistency in guidance publications. At the time of this audit, the terms of reference for the GRC were under development while its linkages had been established in the terms of reference of OSFI's newly established overarching Business Risk and Issues Management (BRIM) committee. The CD Framework currently makes no reference to these governance mechanisms in support of rule-making; hence, consideration should be given to clarifying the roles of the governance structures in place for establishing clearer understanding of their oversight functions over rule-making.

Observations and Recommendations, Continued

Tools / Templates for Guidance Development

CD has a number of tools / template documents available for analysts and management to use as a basis for procedures and guidance development. Based on our review, we noted redundancies in these documents, as they provide similar processes. For example: Appendix E – Rule Making Process Checklist and F – Capital Division Rule Making Process Flowchart in the Framework, the Guideline Development Process Summary, and the Capital Division Rule Making Checklist, are all guidance documents for rulemaking which include duplicate information. There is also the Playbook document intended for outlining eSpace filing that analysts also use as guidance for rule making.

Based on discussions with CD analysts as part of sampled files, we understand that not all staff are familiar with the Framework. Furthermore, it is not clear where the tools / template documents are located in eSpace. We were provided with an eSpace location where CD Banking templates are located; however, neither the Framework nor the tools / template documents for guidance development were found in this eSpace location. Consequently, CD analysts may not be aware of all the existing tools / template documents required for guidance development resulting in the development of additional supporting aids.

Having redundancies in existing documentation and/or documentation not easily accessible could lead to ambiguity in establishing clear expectations and inconsistencies in the application of guidance development which could increase internal operational risk.

Recommendation

CD should update the Framework to reflect structural and organizational changes. The CD should also align the Framework with the principles of the TBS policy instruments, to reflect current CD structure and practices, and to clarify expectations and responsibilities, including the role of any governance mechanisms in place e.g. Guidance Review Committee (GRC). It should also review its existing tools / templates and guidance documents, update them as necessary while reducing redundancies, roll them up into a centralized area within eSpace where they are easily accessible, and provide training / awareness to CD staff on these documents as necessary.

Management Action Plan

The Capital Division agrees with the finding that the Framework needs to be updated to reflect organizational changes. The process will also attempt to consolidate our Framework and procedures into a central reference document or series of documents that could also apply across the Sector. The structure will be dependent on our review of our business process and best format for operational use as well as work with our partners in other Divisions. While some analysts may not be using the current version of the Framework, divisional management is aware of the tools and processes followed in the Capital Division.

We believe this will be beneficial for the onboarding of staff within the Division and better transparency to our business processes.

In addition, the CD will reconcile the Framework with the referenced TBS policy instruments (including TBS Policy and TBS Consultations Guidelines) to ensure it is aligned with the general government approach to policy development.

Observations and Recommendations, Continued

The CD will have the draft update and consolidation completed by September 2020 and finalized ahead of December 2020. Following that portion of the update we will ensure that the continuous review and updates are embedded in our work plans. We will also commit to review the Framework pending the mandate and future work of the GRC. The OSFI Executive has made clear that the use of directed consultation will have limited use under normal guideline development, this change to process will also be included in the revisions to the Framework.

Observation #2: *Formal approval authorities are not adequately explained* (Medium Priority)

As part of the rule making process, analysts often require CD management approvals on various documents including project plans, memorandums, transmittal sheets and responses to written enquiries from stakeholders external to CD.

While the Framework identifies certain activities where approvals are required, it does not adequately explain the level of approval authorities required. Based on our review of CD files and discussions with analysts, they appear to have different interpretations as to whom within CD needs to sign-off on formal documents. This suggests that the CD management approval requirement on rule making activities (pre- and post-guidance publication) may not be clearly outlined in the Framework or understood.

We noted that a centralized reference document (e.g. Approval Authority Matrix) that clearly sets out key activities with corresponding approval levels of reviews and authorization needed from CD management does not exist. Absence of a centralized reference document could create challenges for existing and newly onboarded staff within CD. It could also lead to a lack of understanding of accountabilities. The exercise of approval authority brings personal accountability and responsibility for ensuring that proper investigative and analytical procedures are followed.

With the implementing of Project 'Vu' in the supervision sector, it is expected that as part of future releases, regulation sector will provide input into the applicability and benefits of Vu within its sector. Certain areas of interest in terms of applicability to CD would relate to ensuring a consistent workflow and approval process that can be streamlined within Vu; hence, outlining key activities and associated approval authorities would further help support CD management in exploring its options in terms of how a workflow process within Vu could best support CD with its rule making process.

Recommendation

In order to ensure that sign off authorities are clearly understood at all CD staff levels, CD should develop a reference document that clearly sets out key activities with corresponding approval levels required from CD management. Approval authorities should be clearly defined and communicated to address the current gap.

Management Action Plan

As with Observation #1 – the updating of the CD Framework will include the existing element of approval authorities. The Framework will outline the authorities and responsibilities of each level within the Division and also include Assistant Superintendent authorities.

Observations and Recommendations, Continued

It will also outline these processes for the different types of documents used in the Division (e.g. guidelines, memos, inquiry responses). Such an approval matrix should also be applicable across the Regulation Sector.

The CD will participate in any planned Regulation Sector review of the applicability and benefits of systems such as Project Vu with a goal of improving approval authorities and business systems.

Observation #3: *Information Security*
(Medium Priority)

Pursuant to section 6.4 of OSFI's *Cyber Security Directive for Users* (OSFI Directive), sensitive information must be sent in a secure manner through the use of OSFI's encrypted email channels so that only those authorized can read it. When a security protocol called Transport Layer Security (TLS) is in place at the target email domain(s), emails sent between CD employees and external email recipients are automatically encrypted. OSFI has a list of TLS enabled domains that have been configured to allow TLS communications, and is continually adding to that list. When the TLS option is not available at an organization, OSFI's employees are required to find alternative methods of communication, such as using an OSFI secure USB drive. This secure practice is aligned with OSFI's directive as well as with the Government of Canada's policies on information security.

During the course of the audit it was discovered, through discussions with CD analysts and a review of email communications, that alternative secured methods of communication were not always considered when communicating to external parties as part of the directed consultation process. Additionally, CD lacks a protocol in place regarding the transmission of any sensitive information between CD employees and external email recipients when TLS is not present.

Considering there are no formal business protocols in place to communicate expectations and ensure security requirements are being met with regard to the transmission of sensitive emails, there exists a risk that sensitive information could be mishandled, posing a reputational risk to the organization.

Recommendation

Enhancing CD's current practices and controls around information security should be considered a priority. CD should:

- Establish clear protocols/references regarding the transmission of sensitive emails between CD employees and external email recipients; and
- Promote greater awareness to its staff on OSFI's information security policy requirements.

Management Action Plan

As part of the Framework update work, the CD will include references/links to the TLS protocols so that all staff are aware and able to take respective actions to protect our secure data and OSFI's reputation. The CD will also work with the IT and Cyber Security groups to ensure that all major

Observations and Recommendations, Continued

stakeholders are included under the TLS protocols. Capital Division will work with IT and Cyber Security to ensure stakeholders are informed and are able to adjust their systems before June 2020.

As we have mentioned during the audit most of our material would not be categorized as Protected B so there is less chance that the information falls under the "secure" category. Senior Executive has also directed changes to the Framework to restrict the use of "directed consultations", reducing the level of exposure to the risk identified in the above circumstance.

Observation #4: *Continuous improvement and Quality Controls* (Medium Priority)

Closing of File Checklist

In a 2012 internal audit recommendation Internal Audit had requested that "*The Capital Division should establish a closing file or post-publication "closing of file checklist" whereby management confirms that all relevant information related to rule-making has been filed in the Livelink Explorer and the EDMS Browser to provide a complete record of the rule-making process and decisions made throughout its development...".*

Establishing a closing of file checklist throughout the rule making process provides, 1) a clear decision making trail of relevant "Must-do[1]" documents related to rule-making, 2) continuity on the file, and 3) serves as quality assurance to ensure that the minimum required information relating to rule-making on a specific file has been filed in eSpace.

Based on our review of the files it was determined that the post-publication "closing of file checklist" is not filed in OSFI's electronic filing system (eSpace).

Monitoring Guidance Development Standards

The *Guidance Development Process Summary* checklist outlines the key processes and activities for the rule-making process along with associated timeframes in the implementation of the key processes. The identification of the timelines helps ensure sufficient lead time is taken into consideration for the development/revisions of the guidance for the timely publications to meet industry implementation target dates. While, the established timeline in the guidance are utilized as benchmarks in the planning process by the CD staff for the continuous improvement of the rule-making process, CD management would benefit from monitoring the actual time taken against the established benchmarks/project plans for the key processes to determine improvement opportunities within the rule-making process or for assessing the effectiveness of any implemented innovative processes or tools. The sector priorities/guidances under development/revision are monitored through the quarterly monitoring process however, an analysis at the project level of such information will further help management assess the effectiveness of its operations and identification of lessons learned i.e. whether the lead time was sufficient, consultation period was adequate, or if post-communication and training was timely.

[1] For example, a Project Plan as identified on p. 6 of the Nov 2010 Framework

Observations and Recommendations, Continued

Recommendation

It is recommended that the "closing of file checklist" or a more appropriate quality control mechanism e.g. peer reviews of files be committed and established for ensuring key documents and approvals are retained on files for supporting decisions and in maintaining a corporate memory for future reference.

Management Action Plan

As part of the revisions to the CD Framework, elements relating to quality control and records maintenance will be included to provide greater certainty. The CD will ensure that the electronic version of the "pink folder" process is lodged appropriately by establishing a more clear process.

Observation #5: *Issues log not managed in a coordinated/centralized manner*

(Low Priority)

CD has in place a document titled "Interpretations of OSFI Guidance by the Capital Division" (the Interpretations Guidance), which outlines a process for providing interpretations of OSFI's guidance and regulatory returns for which Capital Division is responsible as well as for defining responsibilities. The document also describes how to document and track queries CD receives. This document applies to banking and insurance enquiries.

In discussion with CD staff, we understand that queries received from external stakeholders follow two streams:

- Queries sent directly to Communications and Engagement Division (CED) at OSFI. In this case CED forwards the query to CD subject matter expert (SME) for input. The SME could then choose to respond directly or provide input to CED for a response. CED tracks the query and follows up with the SME to ensure that a response was sent.
- Queries sent directly to CD. In this case CD assigns a SME to respond to the query.

The Interpretations Guidance document currently in place does not address service delivery standards and timelines or the roles of CED vs CD when queries are received. Furthermore, while that document indicates that a CD staff should update a separate (centralized) tracking sheet (Excel workbook) once an interpretation is provided, this process doesn't appear to be followed for enquiries relating to CD Insurance files, as enquiries for these files are tracked separately in eSpace.

In discussion with sampled CD analysts, they were not familiar with the Interpretation Guidance document.

Not having a complete/updated Interpretations Guidance in place that clearly outlines roles and responsibilities for all stakeholders involved in responding to queries, and that lacks clarity relating to service delivery standard and timeline, could lead to confusion and increases the risks of stakeholder confidence if queries are not answered in a timely manner. Furthermore, queries that are not tracked in a centralized tracking sheet may result in missed opportunities to inform of horizontal opportunities if any, and for continuous improvement.

Observations and Recommendations, Continued

Recommendation

In order to clarify the roles and responsibilities of OSFI's internal stakeholders involved in the query process, and to address the service delivery standards timeline, CD should:

- Update the Interpretations Guidance document to clearly outline the steps that are taken by members of the CED and CD to ensure that queries are responded to within OSFI's service delivery standards.
- Establish delivery standards and timelines, along with centrally tracking and monitoring.
- Provide training / awareness to CD staff on the Interpretations Guidance document process and promoting adherence to the requirements.

Management Action Plan

Similar to the observations above, the Interpretations Guidance will be updated and included in the revisions to the Framework. This will ensure consistency of approach and provide a common understanding to all CD staff. While the CD believes the guidance is clear on roles and responsibilities, the guidance will be further clarified and will be expanded to include an element of service standards that reflect the complexity of the interpretation requested. This work will be completed on the same timelines as referenced above.

Appendix 1 – Observation Ratings

Observations are ranked in order to assist management in allocating resources to address identified weaknesses and/or improve internal controls and/or operating efficiencies. These ratings are for guidance purposes only. Management must evaluate ratings in light of their own experience and risk appetite.

Observations are ranked according to the following:

High priority - should be given immediate attention due to the existence of either a significant control weakness (i.e. control does not exist or is not adequately designed or not operating effectively or a significant operational improvement opportunity).

Medium priority – a control weakness or operational improvement that should be addressed in the near term.

Low priority - non-critical observation that could be addressed to either strengthen internal control or enhance efficiency, normally with minimal cost and effort.

Individual ratings should not be considered in isolation and their effect on other objectives should be considered.