Office of the Superintendent of Financial Institutions Canada

Bureau du surintendant des institutions financières Canada

Internal Controls over Financial Reporting

Internal Audit Report

Assurance Engagement

July 2020

OSFI BSIF

Canada

Table of Contents

Glossary and Abbreviations

AICPA	American Institute of Certified Public Accountants
CFO	Chief Financial Officer
DCFO	Deputy Chief Financial Officer
ELC	Entity Level Controls
ICFR	Internal Controls over Financial Reporting
ITGC	Information Technology General Controls
OSFI	Office of the Superintendent of Financial Institutions
PFM	Policy on Financial Management
TB	Treasury Board
Framework	Five-Year Risk Based Plan for the Assessment, Remediation and Ongoing Monitoring of Internal Controls over Financial Reporting

Background

Context

The Treasury Board's (TB) *Policy on Financial Management (PFM)* came into effect on April 1, 2017, and sets out the requirement for Deputy Heads/Superintendent to establish, monitor and maintain a risk-based system of internal controls over financial reporting (ICFR). ICFR, as defined in the PFM, is "a set of measures and activities that allow senior management and users of financial statements to have reasonable assurance of the accuracy and completeness of the department's financial statements."

More specifically, ICFR are the procedures and mechanisms put in place to provide reasonable assurance that:

a. Records are maintained that support and represent fairly all financial transactions,
b. Recording of financial transactions allows for the preparation of internal and external financial information, reports and statements in compliance with financial management policy instruments,
c. Expenditures are made in accordance with delegated authorities, and unauthorized transactions that could have a material effect on the financial statements are prevented or detected in a timely manner, and
d. Financial resources are safeguarded against material loss due to waste, abuse, mismanagement, errors, fraud, omissions and other irregularities.[1]

An annual risk-based assessment of the system of ICFR is conducted to determine its ongoing effectiveness and the results of the assessment are reported in a separate annex to the financial statements. Monitoring the ongoing effectiveness of the system of ICFR is essential for ensuring potential control weaknesses or any material risks are identified in a timely manner and that prompt corrective action is taken to ensure the reliability of the financial information.

The responsibility for establishing and maintaining the system of ICFR at the Office of the Superintendent of Financial Institutions (OSFI) resides with the Chief Financial Officer (CFO) and the Deputy Chief Financial Officer (DCFO) in the Finance team of the Corporate Services Sector. The *ICFR Core Team* is responsible for planning and conducting the annual risk assessments, and the testing and evaluations of the design and operating effectiveness of key controls. The team consists of the Manager of Financial Policy and Projects, and the Officer of Financial Policy and Project; resources are also complemented through external consultants, if required.

The ICFR framework at OSFI consists of a *five-year risk based plan for the assessment, remediation and ongoing monitoring of internal controls over financial reporting (Framework),* and an annual plan and results report, including action plans for noted exceptions.

The multi-year Framework is a living document, setting out the responsibilities of OSFI with respect to the monitoring and maintenance of the system of ICFR. The Framework defines the system of ICFR to include consideration for controls at the following levels:

- **Entity Level Controls (ELC)** - are defined as those controls which impact the organization at the highest level and impact the overall effectiveness of the system of internal controls. They are often referred to as the "tone from the top" type of controls.
- **Transaction Level Controls**- are controls embedded in the day to day recording of financial information (e.g. accounts payable, accounts receivable, revenue or expense). The performance and effectiveness of these controls is a factor of the entity level control effectiveness.
- **Information Technology General Controls (ITGCs)** - are similar to entity level controls, set the tone for the IT environment as a whole, The primary focus is on logical access and change management controls within systems critical to financial management and reporting.[2]

All three levels of control operate together to collectively reduce the risk to the achievement of ICFR objectives.

Continued on next page

[1] As per the Treasure Board *Policy on Financial Management*, April 2017.
[2] OSFI's *Five-Year Risk Based Plan for the Assessment, Remediation and Ongoing Monitoring of Internal Controls over Financial Reporting*, fiscal years 2014/15 to 2018/19, pages 3-5.

Background, Continued

The Framework for the fiscal five-year period 2014/15 to 2018/19 identifies 11 key transactional processes based on financial statement risk assessments, which forms the basis for establishing a rotational methodology for the assessment of the key controls in a given year for the entity level, transactional level and ITGC level. The Framework identifies that key processes rated as *high* risk be subject to operational testing each year, and processes rates as *medium or low* risk be subject to rotational testing over a two year period.

Monitoring, per the Framework, is defined as the ongoing evaluation of the system of ICFR, which can include testing of controls and reporting of deficiencies. It is intended to ensure that internal controls continue to operate effectively and as designed without exception. Hence, monitoring includes the ongoing assessment of both the design and operation of controls, and taking necessary actions to address any identified weaknesses.

The focus of the audit was to provide assurance on the adequacy and effectiveness of the ongoing monitoring of the system of ICFR at OSFI. This entailed a review of the framework and methodology for assessing key processes, including review of the results of the testing documentation for the entity level controls, and the eight business processes under review for the period of April 1, 2018 to March 31, 2019, which included 40 key controls and ITGCs.

An audit of ICFR was recommended by OSFI's Audit Committee and approved by the Superintendent for inclusion in the OSFI 2019-20 Internal Audit Plan.

Objective

The objective of the audit was to assess the extent to which OSFI's ICFR Framework was aligned with the Government of Canada policy and guidelines; the adequacy and effectiveness of the core elements of the ICFR program, including any supporting operational procedures and practices; and the governance and monitoring mechanisms.

Scope

The audit focused on an assessment of the key ICFR program elements including the ongoing monitoring and testing of the ICFR program through interviews and reviews of documentation to ensure alignment with the established framework for the fiscal year 2018/19. The audit did not assess the design and operating effectiveness of individual key controls.

Testing documentation of the following eight business processes in scope for the fiscal year 2018/19 monitoring plan were reviewed, along with the corresponding number of key controls in the brackets below:

- Accounts Receivable – Cash Receipts (4)
- Contracting (Procurement) (6)
- Month End/Year End Accruals (5)
- Revenue – Base Assessments (4)
- Revenue – Pension Plan Assessments (4)
- Payroll (10)
- Accounts Payable – Invoice & Payment (4)
- Quarter End/Year End Disclosure (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 TB's *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.

Results of the Engagement

Overall, OSFI's Finance Team has established a comprehensive Framework for the ongoing monitoring of the ICFR, which outlines foundational elements supporting how key activities are to be carried out on a cyclical basis in alignment with the requirements of the Treasury Board *Policy on Financial Management* and provides reasonable assurance over the integrity of the financial information.

Our audit found that the approach towards Entity Level Controls (ELC) could be more risk-based focused in the design and operating effectiveness testing of key controls that have a material impact on OSFI's environment. Additionally, the Finance Team would benefit from reviewing and updating their controls testing activities to ensure proper alignment with the Framework, and in ensuring appropriate documentation and quality standards are maintained within testing records. Lastly, the ICFR Framework should also be reviewed and updated to include parameters for ensuring that prompt corrective action is taken when control deficiencies are noted, guidelines for ensuring that the extended sampling of exceptions is risk based and clearer articulation of the roles and responsibilities of the ICFR governing bodies.

Management Response

Management would like to thank Internal Audit for their collaborative approach and constructive feedback through this Audit engagement. The recommendations offer meaningful opportunities to build on a strong ICFR foundation. The report provides improvement opportunities that could help strengthen the ICFR framework and ensure OSFI's continued compliance with the Treasury Board *Policy on Financial Management*.

Management Action Plans for each individual audit observation are outlined in the relevant sections. The evaluation of specific components of the ICFR Framework will involve the Operating Committee, the internal governance body that oversees OSFI's ICFR work; more specifically, the committee will review and approve any ensuing amendments to the Framework.

As per the underlying action plans, an updated Framework will be in place for the 2021-22 testing year. Management has developed resource contingency plans to mitigate key person risk and thus the risk of implementation delays.

Observation and Recommendation 1: Entity Level Controls

High Priority Observation

Entity level control (ELC) assessments do not follow a risk-based approach to identifying relevant key controls for design and operating effectiveness testing.

Entity level controls (ELC) are controls that have a pervasive impact across an organization, department, or at a cost centre level and thus can have a direct or indirect impact on the overall effectiveness of the system of internal controls, including an impact on the reliability of controls at the transactional process level if not present and functioning effectively.

For the period under review, the Framework classified ELCs as *low risk* based on the results of the design assessment and hence were subject to testing on a rotational two-year period. The Framework for future fiscal periods has since been updated to require *low risk* rated processes, including ELCs, to be assessed every three years instead. The Framework, however, stipulates that "*any control exceptions or changes in related risks rose during the design assessment or operational testing could elevate the risk priority to moderate or higher".*

ELC Assessments

The ICFR team conducts the design assessment of the ELCs against 204 best practices, in alignment with the COSO framework principles under the five elements of *control environment, risk assessment, control activities, information and communication, and monitoring*. The ICFR team's evaluations against the best practices was conducted through interviews of senior management, and reviews of OSFI documentation.

The assessments of the ELCs currently do not sufficiently support an overall effectiveness conclusion, due to gaps in the methodology and the reporting of the results. For example, of the 204 best practices applicable to OSFI, 74 did not describe how OSFI demonstrated them in practice and 120 of the best practices contained no assessments of operational effectiveness.

The basis for determining what is considered relevant for governance reporting is also not clear. The ELC assessment identified 17 instances where processes either lacked in comparison to best practices or were deficient in design, however only one deficiency was reported to the governance committee i.e. the pause on the implementation of the organization-wide risk assessment while others such as the lack of communication regarding violations of expected behaviour, gap in training and setting expectations around internal control responsibilities were not escalated for governance reporting. As well, the aggregate level of reporting, rated as "good" with 187 of 204 best practices being present suggests an equal weighting of all best practices, when certain practices are likely more applicable and significant to OSFI's control environment. Based on the number of departures from best practices not reported to the governance body, the best practices should be evaluated for applicability and whether or not they necessitate assessments in relation to OSFI's environment.

While ELCs can have an indirect and pervasive impact on the control environment of the organization, such as tone at the top (i.e. communication of expectations through standardized policies and procedures) and hiring practices (establishing high ethical standards in hiring practices and termination procedures), ELCs implemented at a greater precision to monitor specific risks can have a more material and direct implication on the likelihood of detecting and preventing financial misstatements such as monthly variance analysis. Without using a risk-based approach to identifying key controls and implementing corresponding test procedures for assessing operating effectiveness of ELCs, material control weaknesses that have a direct impact could go undetected.

Continued on next page

Observation and Recommendation 1: Entity Level Controls, continued

Recommendation

OSFI should establish a risk-based approach to its ELCs by evaluating which of the 204 best practices pose the highest level of relevance to OSFI's environment and identifying associated key controls, and establishing corresponding test procedures for assessing operating effectiveness for their ongoing functioning. A structured, repeatable and documented process should be established, and the ongoing monitoring and reporting should occur on the basis that is appropriate for the level of risk that the controls present from both the results of its design and operating effectiveness.

Management Action Plan

The Finance team will undertake a full review of OSFI's approach, methodology and processes for assessing ELCs. The review will specifically consider the above observations and aim to deliver a risk-based approach for identifying relevant key controls and establish a structured and repeatable process with appropriate monitoring / reporting requirements. The Finance team will complete this review by December 2020. The results of the review and proposed revisions to OSFI's ELC approach / methodology will be presented to the Operating Committee for review and approval in Q4 (by March 31, 2021).

The revised ELC methodology and processes will be adopted for testing after April 1, 2021.

Observations and Recommendation 2: Transaction Level Controls and ITGCs

Medium Priority Observation

Risk and control matrices supporting process flowcharts are not validated annually with business owners and some test procedures lacked demonstrated evidence of performance to support conclusions for both transactional level controls and ITGCs.

OSFI's *Five-Year Risk Based Plan for the Assessment, Remediation and Ongoing Monitoring of Internal Controls* (Framework) outlines how ICFR activities are to be carried out. This includes the assessment of key controls, the monitoring of the system of ICFR, the responsibilities of ICFR at OSFI and the testing plan for entity level and transaction level controls and IT general controls (ITGCs).

It was expected that ICFR business processes would be tested for design and operating effectiveness and that activities would be carried out in accordance with the Framework. Standardized templates have been established outlining key controls, test procedures, and for documenting the results of the business process testing.

In validating ICFR team's 2018-19 testing activities, the following exceptions were noted:

- As part of the annual ICFR activities, in order to ensure the continued validity of the key controls, the ICFR team is required to validate the process flowcharts and corresponding risk and control matrices with the process owners, and update accordingly. The risk and control matrices were not validated with the process owners for the 2018-19 fiscal year, and final confirmation to validate accuracy on the revised process flowcharts were not documented from all business process owners.

- A review of the testing activities identified a lack of documented evidence to demonstrate the completion of five specific test steps found across eleven key controls over three business processes. The ICFR Core Team indicated that the reason for some additional test procedures not being performed for four other business processes was due to the testing steps not being designed appropriately. *Details of the specific individual control observations have been provided to management to address.*

- Documented, standardized testing procedures and a mechanism for demonstrating performance were found to be lacking for user access control testing and the testing of specific key application controls.

Without updating risk and control matrices and demonstrating that testing procedures were carried out, the ICFR assessments may fail to detect control deficiencies and ensure controls are relevant and updated with any new risks identified to the business processes. These deficiencies do not necessarily imply that the ICFR team is unaware of the risks that exist within processes or that sufficient testing was not performed. Given that established mechanisms in place were not followed to demonstrate these validations, we were unable to determine whether all relevant information has been considered in developing the risk-based approach to testing key controls and whether the operating effectiveness testing is sufficient to determine the ongoing effectiveness of some of the transactional level controls and ITGCs.

Recommendation

The ICFR validation and testing activities are fundamental to providing reasonable assurance that process descriptions remain current, risks are identified, and key controls are assessed for design and operational effectiveness. Specifically, ICFR Team should:

- validate the risk control matrices with the business owners for completeness and accuracy along with obtaining confirmations on process flowchart changes annually, and

Continued on next page

Observations and Recommendation 2: Transaction Level Controls and ITGCs, continued

Recommendation, continued

- review and update the testing procedures to ensure they are appropriately designed to test key control objectives and ensure test results are sufficiently documented to demonstrate performance and support conclusions for key business process controls and ITGCs.

Management Action Plan

The Finance team has already amended the validation steps / activities for the fiscal year ending March 31, 2020. Business process owners were asked to validate the risk control matrices and process flowcharts to ensure completeness and accuracy. To ensure the practice is maintained on a go-forward basis, a checklist has been created and duly implemented to ensure the systematic review and validation of both the control matrix and process flowcharts by business process owners during each testing cycle.

Furthermore, the Finance team completed a review of the business processes that were tested during the fiscal year ending March 31, 2020 to ensure the testing procedures aligned with the controls; the remaining processes (i.e., those not scheduled for testing during the year ending March 31, 2020) will be reviewed by March 31, 2021.

The ICFR Framework will be updated to incorporate changes resulting from the above steps. This will be done as per the timelines under the Management Action Plan under Audit observation #3 (by June 30, 2021).

Observation and Recommendation 3: Governance Roles and Reporting

Medium Priority Observation

Greater clarity on the role of governance bodies and corresponding reporting requirements is required. Reporting of control exceptions to governance bodies lack sufficient information for exercising appropriate oversight and support effective decision-making.

The Treasury Board's *Policy on Financial Management* (PFM) requires that prompt corrective action be taken when control weaknesses and material risks are identified in the system of ICFR. The established ICFR Framework addresses reporting on control exceptions and observations noted during ICFR testing to be presented to the appropriate governing bodies for review and approval, where required.

Control Exceptions Reporting

Outlined in the annual financial statement risk assessments is the criteria for determining the impact of previously identified control exceptions on the risk ratings of the financial accounts and related business processes for establishing the extent of testing required (e.g. high risk processes to be tested annually). Criteria for establishing the significance of control weakness as low, moderate or high including corresponding timeframes for remedial action (e.g. deficiencies categorized as high risk to be addressed within a year) are established to support this analysis. The Framework, however, is silent on this established criteria for control exception risk prioritization within the financial statement risk assessment worksheet.

Our review of the control weaknesses reported, noted the following:

- Five control exceptions/observations were noted for fiscal year 2018/19 and while the exceptions/observations, with management action plans, were reported in the *ICFR 2018-19 Final Report* and in the presentation to the appropriate oversight body, the Operating Committee (OC); the reporting did not include assignment of risk ratings to the individual control exceptions or the associated timelines for remedial actions.

- The Framework stipulates that more than one control exception results in the control having operationally failed and requires reporting to the OC. A review of the testing results and *ICFR 2018-19 Final Report* revealed that while an exception was noted relating to the control testing, the full extent of the control failure was not reported or highlighted in the presentation to the oversight body, the OC.

Without complete reporting on the extent of the noted exceptions and on the significance of the identified control deficiencies through established risk ratings and corresponding acceptable timelines for remediation, the program risks not providing sufficient and relevant information to the governance bodies to effectively execute its oversight function.

Governance Roles and Reporting

Although the ICFR Framework for the year under review outlines the requirement for the noted exceptions to be reviewed by the Operating Committee, the Framework lacks clearly articulated requirements for reporting and approvals of other key governance documents such as the *Five-Year monitoring plan,* the *ICFR final report*, and the *annex to the financial statements*. This lack of clarity could result in key ICFR documents not being reviewed and approved by the appropriate level of senior management and OSFI's governing bodies not being aware of risks to the ICFR program to appropriately exercise their oversight function.

Recommendation

It is recommended that reporting to governance bodies should entail greater level of detail on the extent of noted exceptions, including identifying the level of risk associated with the exception and corresponding timelines for remediation to allow for effective oversight and

Continued on next page

Observation and Recommendation 3: Governance Roles and Reporting, continued

Recommendation, continued

decision-making. Additionally, the Framework should be reviewed and updated to clearly articulate the roles of the governance bodies and respective reporting requirements, including approvals for the five-year monitoring plan, the final results report and the annex to the financial statements.

Management Action Plan

Management agrees that the level of detail surrounding exception reporting could be expanded and, on a go-forward basis, will make a concerted effort to do so.

The Finance team will engage the Operating Committee on the role of the governance bodies and reporting requirements to allow them to exercise their oversight responsibilities. This will help inform the reporting of exceptions, including identifying the level of risk, and the timelines for remediation. This work will be completed by the fourth quarter of the fiscal year ending March 31, 2021.

Following this step, the ICFR framework will be reviewed and updated to clearly articulate the roles of the governance bodies and respective reporting requirements, including approvals for the five-year monitoring plan, the final results report and the annex to the financial statements. The revisions will provide additional information on which documents require CFO or Operating Committee approval. The updates to the framework will occur by the end of the second quarter of the 2021-22 fiscal year and will be presented to the OC in the following quarter (Q3).

Given key person risk within the Internal Controls function (i.e., limited resources & staffing challenges), third-party resources will be engaged by July 31, 2020 to mitigate the risk of delays to interim projects steps & deliverables.

Observation and Recommendation 4: Risk-Based Sampling

Medium Priority Observation

Consideration should be given to revising the sampling methodology and utilizing computer assisted technology in testing to focus on high risk areas.

The testing of key controls is a key activity of the ICFR program and requires a sampling methodology that is designed appropriately. The ICFR Framework clearly outlines a sampling methodology for both initial testing, testing exceptions and extended sampling that is designed based on guidance from the American Institute of Certified Public Accountants (AICPA). It was found that although the sampling was applied according to the framework in most cases, when exception testing was required the methodology for drawing the extended sample from the population was not targeted to specific risk areas to provide greater assurance on operational effectiveness. For example, when extending the sample selection for the Procurement (Contracting) business process, 60% of the extended sample did not relate to the area where the exception was discovered. Without targeting the extended sample to the area where the exception was uncovered, the testing results lack insight into the actual functioning of the key controls, leading to unidentified errors or conclusions on operating effectiveness.

The updated Framework for future fiscal period outlines consideration for technological tools to assist in focused transaction testing and an exploration of the benefits of statistical sampling of accounts payable transactions as OSFI moves towards the implementation of a new financial analytical tool. As this initiative is in its infancy, significant progress has not been made to date.

Recommendation

It is recommended that the ICFR team review and revise the sampling methodology to ensure that extended sample testing is focused on the area where exceptions are noted and consider prioritizing the exploration of computer assisted technology to aid in control testing. Moving to computer assisted technology for sampling may allow the ICFR team to focus on areas of greater risk in testing key controls for operational effectiveness.

Management Action Plan

The Finance team will complete a review of the appropriateness of the sampling methodology by the fourth quarter of the fiscal year ending March 31, 2021. The assessment will be guided by the audit recommendation and keep in mind the following core principles:

- The testing of ICFR requires evidence of controls occurring without exception throughout the period tested.
- A test of controls is made irrespective of the dollar amount of the underlying business transaction.
- If an error is encountered in a test of controls, they will expand the sample size and conduct further testing.
- If additional errors are found, they will consider whether there is a systematic controls problem that renders the controls ineffective, or if the errors appear to be isolated instances that do not reflect upon the overall effectiveness of the control in question.

Separately, The Finance team will explore the possibility of leveraging computer-assisted technology for sampling purposes. This review for will also be completed by the fourth quarter of the fiscal year ending March 31, 2021.

The results of these assessments will be presented to the OC for review and approval by June 30, 2021.

Observation and Recommandation 5 : Documentation Maintenance

Low Priority Observation

Quality issues were noted within ICFR documentation, including dated information, misaligned testing procedures and lack of instructions for re-performance.

The ICFR Team has developed an extensive set of templates for documenting the results of the annual activities. The documentation serves to record the results of the testing, any noted deficiencies and observations and the overall conclusion on the operating effectiveness of each control.

For all business processes, testing templates were consistently utilized; however, data quality issues were noted within the worksheets, including discrepancies in the consistency of recorded information when in two locations, outdated examples/samples, incorrect testing dates, and misaligned test procedures to control objectives (noted in above observation #2). *Details of the specific individual observations have been provided to management to address.*

The documentation maintenance issues were not found to have impacted the ICFR testing results and conclusions; however, lack of quality in maintaining documentations may result in the results of the ICFR activities not being sufficiently supported or entailing an appropriate level of rigour for maintaining its effectiveness.

Recommendation

It is recommended that the ICFR team and management ensure sufficient level of reviews are conducted to maintain higher levels of quality standards in documentation for ensuring accuracy of recording information, including relevant and current supporting examples, relevant test procedures and sufficient level of instructions to allow for re-performance.

Management Action Plan

The Finance team has already completed a review of the testing documentation used for the transactional business processes that are in scope for the fiscal year ending March 31, 2020. More specifically, the documentation was reviewed to ensure accuracy of recording information, relevant and current supporting examples, relevant test procedures and sufficient level of instructions to allow for re-performance. The remaining testing documents (i.e., those applicable to processes not in scope in 2019-20) will be reviewed and updated prior to December 2020. To prevent data quality issues in the future, these templates and documentation will be subjected to a similar review during each testing cycle that they are used.

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.