Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada
Canada

Guide to Ongoing Monitoring of Internal Controls Over Financial Management

Published: 2020-05-04

Published by Treasury Board of Canada, Secretariat
90 Elgin, Ottawa, Ontario, K1A 0R5, Canada

Catalogue Number: BT22-224/6-2020E-PDF
ISBN: 978-0-660-34566-6

This document is available on the Government of Canada website, Canada.ca

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Guide de surveillance continue du contrôle interne en matière de gestion financière

Guide to Ongoing Monitoring of Internal Controls Over Financial Management

1. Date of publication

This guide was shared with departments on November 22, 2019.

This guide replaces the Treasury Board Guideline for the Policy on Internal Control

2. Application, purpose and scope

This guide applies to the organizations listed in section 6 of the *Policy on Financial Management*.

The purpose of this guide is to support departments and agencies with the ongoing monitoring of internal controls and the maintenance of an effective system of internal controls over financial management (ICFM).

“Financial management” is defined in the *Policy on Financial Management* as:

> a continuum of finance-related activities undertaken to ensure sound and prudent use of public funds in an effective, efficient and economical manner.

This guide elaborates on the *Policy on Financial Management*. It does not contain any new mandatory requirements. Examples and tips are included for reference and may not apply to all departments or situations.

Readers of this guide are encouraged to refer to the *Guide to Internal Control Over Financial Management* to better understand:

- the basis of internal control
- key accountabilities and policy requirements
- the scopes of internal controls over financial reporting (ICFR) and ICFM

Suggestions to improve this guide should be sent to the Financial Management Policy Division of the Office of the Comptroller General at fin-www@tbs-sct.gc.ca.

3. Overview of ongoing monitoring of internal controls over financial management

3.1 Defining ongoing monitoring of internal controls over financial management

With the introduction of the *Treasury Board Policy on Internal Control* in 2009, departments have been:

- assessing their ICFM
- focusing specifically on ICFR
- Departments have subsequently:
    - identified the accounts, associated processes and systems that had the highest risk of causing financial misstatement
    - established plans to document, assess and improve key controls

As noted in the *Policy on Financial Management*, the requirement to maintain a reliable system of ICFM remains in force.

Internal controls are affected by changes to roles, processes, systems and structures. New controls may need to be introduced, and existing controls may need to be amended. Departments must therefore conduct ongoing monitoring of their internal controls to ensure that they remain effective.

Ongoing monitoring of internal controls using a risk-based approach involves:

- assessing the design and operating effectiveness of the controls regularly in accordance with the monitoring plan
- determining whether any actions need to be taken to address weaknesses
- Ongoing monitoring of internal controls begins after a department has completed its initial control assessment. The control assessment involves:
- documenting the controls
- testing for design effectiveness and operating effectiveness
- developing a management action plan to correct gaps or weaknesses

Ongoing monitoring allows the deputy head (DH), chief financial officer (CFO) and senior departmental managers (SDMs) to confirm that:

- a system of ICFM exists
- the system is reliable
- actions have been taken to improve controls

3.2 Internal controls over financial management and internal controls over financial reporting

The DH, CFO and SDMs are accountable for the system of ICFM, including the ongoing monitoring and maintenance of ICFM in their department. The DH and CFO are specifically required to report on the status of the system of ICFR through the Annex to the Statement of Management Responsibility Including ICFR.

When conducting ongoing monitoring, the department must:

- define the functions and processes relevant to its organization
- identify the key controls related to financial management according to risk

Effective ICFM:

- provides reasonable assurance of the department's sound and prudent use of public funds
- improves the effectiveness of financial management processes
- complies with statutory, regulatory and policy requirements

3.3 What are the benefits of ongoing monitoring?

The key benefit of ongoing monitoring of financial management processes and controls is that it makes it possible to detect key risks and changes in the control environment. Ongoing monitoring:

- allows management to adapt or introduce controls to ensure that risks are mitigated
- informs the planning and prioritizing of financial management activities by offering insight into the efficacy of the processes and controls in place

More specifically, ongoing monitoring helps departments:

- highlight gaps in control that could affect the achievement of business objectives
- apply leading practices to bridge identified gaps and mitigate risks
- increase staff awareness of the business unit's objectives and the importance of following established processes and controls
- increase the confidence in and the understanding of the information provided to management in support of decision-making
- improve the development of training materials for employees through the use of well-documented business processes
- ensure that employees fulfill their responsibilities and understand how their roles and responsibilities fit with others in the organization
- reduce non-compliance with laws and policies

Ultimately, a strong system of ICFM:

- improves the department's ability to meet its financial management objectives
- helps inform other oversight activities, including:
- internal and external audits (Office of the Auditor General)
- evaluations

3.4 What are employee's and departments' responsibilities in the area of ongoing monitoring?

Employees responsible for ongoing monitoring should:

- maintain accurate, up-to-date descriptions of the business process controls, information technology (IT) general controls and entity-level controls
- consider whether internal controls are designed effectively when changes occur in the organization or in the external environment
- assess whether controls continue to operate effectively

Departments should:

- have a consistent approach to ongoing monitoring
- use other forms of oversight for their controls, such as:

- internal audit (IA)
- evaluation
- assessments of corporate and operating risk

4. Governance structure for ongoing monitoring

According to subsection 16.4(1) of the *Financial Administration Act* and subsections 4.1.6, 4.2.8, 4.2.9, 4.2.10, 4.3.6 and 4.3.7 of the *Policy on Financial Management*, the DH, CFO and SDMs have roles and responsibilities with regard to implementing, maintaining, assessing and ensuring a risk-based system of ICFM. These roles and responsibilities include activities for ongoing monitoring.

Departments must document stakeholders' roles, responsibilities and accountabilities of so that they know what is expected of them in terms of:

- designing and implementing ongoing assessments
- developing and implementing corrective actions
- reporting on the status of internal controls
- reviewing ongoing assessments
- participating in governance committees

SDMs should be informed that they are accountable for the system of ICFM under their area of responsibility (refer to section 4.1 of the *Guide on ICFM* for information on accountabilities and policy requirements). This responsibility can be reinforced by including ICFM expectations in SDM's performance measurement agreements. In addition, departments can confirm the effectiveness of internal controls annually with the appropriate SDMs.

Departments should review the assessment program for ICFM with SDMs regularly (for example, annually). This discussion can include:

- the proposed plan for ongoing monitoring of ICFM
- how the department's operational areas are supposed to participate in the assessment program for ICFM
- the results of the assessment program for ICFM
- the implementation of action plans to address weaknesses in control

The CFO determines which monitoring activities are ongoing. Such activities can include:

- providing progress reports to departmental executives
- informing the DH about the status of ICFM
- reporting on the status of ICFR in the annual Annex to the Statement of Management Responsibility Including ICFR

Departments should also report to their departmental audit committee (DAC) on the system of ICFM, at least annually, and include:

- key risks that impact the system of ICFM

- the ongoing monitoring plan
- the results of assessments

This reporting would support the DAC by providing a comprehensive view of the status of the system of ICFM. The DAC would then be able to view the results along with other audit and evaluation findings.

5. Approach to ongoing monitoring

The suggested approach to ongoing monitoring of ICFM has 5 steps. These steps:

- are coordinated by the department's internal control team (ICT)
- involve various stakeholders in the department

This approach is designed to:

- assure the DH and the CFO that the department's system of ICFM is effective
- support the development of the Statement of Management Responsibility Including ICFR

The approach to ongoing monitoring allows for updates to the scope when there are changes to the organization or legislative policy requirements. Figure 1 shows the 5 steps.

Figure 1: ongoing monitoring approach for ICFM

▶ Figure 1 - Text version

The Treasury Board *Guide to Internal Control Over Financial Management* provides more details on requirements for ICFR.

The 5 steps are as follows.

Step 1: Develop and update the risk assessment to determine which business processes, IT systems and entity-level controls are in scope. Doing so informs the nature and extent of the testing.

Step 2: Develop and update the ongoing monitoring plan, which outlines the timing and frequency of the assessment of:

- business process controls
- IT general controls
- entity-level controls

For more details on the various categories of controls, refer to Appendix A.

Step 3: Complete the assessmentof internal controlsaccording to the ongoing monitoring plan.

Step 4: Capture the results and remediation actions from the assessment.

Step 5: Develop the internal and external reports to include the results of the assessment and recommendations for remedial actions. Internal reporting is expected for ICFM that encompasses ICFR. However, external reporting is only required for ICFR.

Details on each step follow.

5.1 Step 1: develop and update the risk assessment

Departments should use a risk-based approach to determine how often processes and controls need to be monitored to ensure that the system of ICFM is effective. Using a risk-based approach results in a more effective use of limited resources.

Higher-risk areas usually require:

- more in-depth documentation
- more controls
- the use of preventive controls or a mix of preventive and detective controls (detective controls may be sufficient for lower-risk areas)
- more frequent testing

A full risk assessment of the department's ICFM is beneficial to:

- understanding where the key risks are
- determining the focus of the assessment

A full risk assessment of ICFM is required only once every 3 to 5 years. Environmental scans can be conducted during the intervening years to determine whether the ongoing monitoring plan requires adjustments. Figure 2 shows an example of a 5-year risk assessment schedule.

Figure 2: example of a 5-year risk assessment schedule

▶ Figure 2 - Text version

Each department determines the timing of each component of its ongoing monitoring plan and of its risk assessments. The time frame may be influenced by:

- how much personnel, processes or underlying IT systems have changed
- how much the department's operations and operating environments have changed or are expected to change
- a cost-benefit analysis of whether to conduct a risk assessment

Departments may also consult the *Framework for the Management of Risk* for:

- additional insight into risk management principles
- guidance on the effective management of organizations

Conducting a full risk assessment

A full risk assessment involves 2 key activities:

1. data-gathering
2. risk assessment

1. Data-gathering

Data-gathering involves:

- examining documentation
- questioning Business Process Owner (BPOs)

For data-gathering to be effective, the ICT needs to:

- learn about the business processes and the operating environment
- meet with individuals outside the CFO organization, including:
    - program managers
    - human resources personnel
    - IT personnel

At a minimum, the ICT should consult with the BPOs to confirm whether any of the following have changed significantly:

- the business processes
- the staff who perform the controls
- the systems that support the business processes

It is a good practice to meet with a sample of SDMs to gain an understanding of the department's:

- strategic direction
- potential organizational changes
- concerns with respect to ICFM

In addition to consulting the BPOs, the ICT should also review background documentation, such as internal and external reports. The reports may contain useful information to inform the risk assessment. Examples of documentation that may inform a risk assessment include:

- ICFR and ICFM reports (status updates, action plans, assessment results)
- audit reports from IA, the Office of the Auditor General, and the Office of the Comptroller General
- changes to departmental or Treasury Board policies, government accounting standards, or to the departmental operating structure
- pre- and post-payment verification reports
- Management Accountability Framework results
- departmental financial statements
- the Annex to the Statement of Management Responsibility Including ICFR
- profiles of corporate or enterprise risks

The data-gathering exercise may reveal new business processes that result from a program or policy change. If that is the case, the ICT will need to:

- assess the risk associated with these new business processes
- incorporate the processes into their ongoing monitoring plan

Together, the ICT and IA can ensure the most effective use of resources and minimize the impact on stakeholders. Specifically, the ICT and IA can:

- share information about the assessments that they need to perform
- identify where joint assessments can take place
- exchange control testing results when determining the scope of their audit engagements

In addition, the ICT can use IA results if the objectives and the approach of the controls assessment are sufficiently aligned (for example, IA may be testing operational effectiveness on the same control points that the ICT wants to examine).

Industry organizations, such as the following, also offer good practices in terms of documenting and testing of controls:

- the Committee of Sponsoring Organizations of the Treadway Commission
- the Institute of Internal Auditors

2. Risk assessment

After the data-gathering is completed, the department conducts a risk assessment of the key business processes and systems to assess:

- the likelihood of the risk materializing
- the impact of the risk on financial reporting and financial management

If risk assessments have been conducted for the process in the past, the department can use the same tools and templates. If a new process is being introduced (for example, CFO attestation for Cabinet submissions), a new risk assessment template will be required.

The ICT should consider materiality when assessing the impact of a risk occurring. Subsection A.2.2.2 of the *Directive on Accounting Standards* (GC 1010 Financial Statements Concepts (Materiality) outlines various approaches to calculating materiality. The ICT should also consider non-financial impacts that may occur if a transaction or process is subject to public scrutiny (for example, travel and hospitality expenses).

The likelihood of a risk occurring depends on:

- risk factors inherent in the process
- previously identified issues in the process

Mitigating risks involves assessing a process against the following qualitative risk factors.

Inherent risk factors

- materiality: a higher aggregate value may increase the risk of a material error to the financial statements
- volume: more transactions may increases the risk of error
- complexity: a complex transaction may increases the risk of error
- homogeneity: a more homogenous population may decreases the risk of error
- susceptibility of loss due to errors or fraud within the process: a higher susceptibility of loss increases the risk of error
- judgment: a higher reliance on judgment increases the risk of error
- other risk factors: some transactions are not material in terms of dollars but they may:
    - be sensitive
    - have an impact on management decision-making

Risk of control failure

- degree of automation: in general, manual controls are more prone to error than automated controls
- history of error: a process that has a history of errors has a higher risk of control failure and would be considered higher risk
- Sources of information about the history of error include:
    - results of previous internal control assessments and audits

        - results of other monitoring activities (for example, account verification, monthly monitoring, year-end monitoring, corporate accounting reviews)

As the department transitions from ICFR to ICFM, additional risk factors should be addressed, such as:

- the susceptibility of overspending authorities
- the susceptibility to lapsing funds
- the risk of making poor resource allocation decisions

Taking these factors into consideration can result in new control activities for ICFM. Examples of the end result of such activities are:

- salary forecasting is reliable and can be used to make decisions on allocating resources
- commitment information is accurately recorded in the departmental financial management system as part of the operating expenditures process

These factors can also have an impact on the annual assessment. For example:

- A department that lapses its budget year over year by significant amounts might need to assess its forecasting processes
- A department that regularly seeks amendments to its expenditure authorities related to Treasury Board submissions might need to assess its costing processes and controls

The results of the risk assessment should be documented and validated by the CFO. The assessment will serve to prioritize elements of the ongoing monitoring plan.

Table 1 gives an overview of the roles and responsibilities in Step 1, broken down by the "RACI" approach, [1] which stands for:

- responsible
- accountable
- consulted
- informed

Table 1: key stakeholder responsibilities in conducting a full risk assessment

Activity	Responsible	Accountable	Consulted	Informed
Data-gathering	ICT	CFO	BPO, IA and CRT [2]	CFO, DAC, DH, IA and SDM
Risk assessment	ICT	CFO	BPO, IA, CFO and CRT	CFO, DAC, DH, IA and SDM

Undertaking an annual environmental scan

In the years between conducting full risk assessments to creating the ongoing monitoring plan, the ICT should conduct environmental scans to determine whether the ongoing monitoring plan needs to be updated.

An environmental scan involves determining whether there have been significant changes to the personnel, process or systems that would warrant a change to the ongoing monitoring plan. An environmental scan involves the same activities as a full risk assessment (data-gathering and risk assessment), but it may be less intense or comprehensive. An environmental scan should include the following activities:

- reviewing documents that affect the department's financial management
- surveying BPOs
- following up on the management action plan for previously reported control weaknesses

Table 2 shows the differences between a full risk assessment and an environmental scan.

Table 2: differences between full risk assessment and environmental scan

Full risk assessment	Environmental scan
Interview BPOs	Survey BPOs
Obtain updates on the management action plan	Obtain updates on the management action plan
Examine relevant documents	Review recent ICFM reports and audit reports related to processes in scope
Consult IA	Obtain recent audit reports
Hold a working session with BPOs to assess risk	Consult with BPOs as needed

The result of a full risk assessment is an updated ranking of:

- the key business and IT processes
- the entity-level controls

The result of the environmental scan and changes to the ongoing monitoring plan should be documented. The amended plan should be submitted to the CFO for consideration. SDMs and the DAC should also be kept informed of the changes to the ongoing monitoring plan. IA should be included in discussions to update the plan so that it can coordinate testing activities.

5.2 Step 2: develop and update the ongoing monitoring plan

When developing the ongoing monitoring plan, the department should:

1. determine the duration and timing of assessments
2. determine the resource model
3. develop a plan

The intent of this step is to update the plan and ensure that it:

- continues to be valid
- reflects changes to the organization, including new processes or systems identified earlier

1. Determine the duration and timing of assessments

The ongoing monitoring plan is the basis for detailed, future ICFM assessment work plans. The department determines the duration of the ongoing monitoring plan, which may be from 3 to 5 years. The timing and frequency of the assessments take into account factors such as:

- critical emerging events, including proposed strategic plans
- resource constraints
- the costs and benefits of the assessment compared with the risks associated with the process
- the status or results of remediation action plans (if remediation has not yet taken place, there may be little value in performing the assessment)
- audit findings that may have an impact or that may provide further evidence of the effectiveness of controls
- other parallel financial reviews or initiatives

The plan should be approved by the CFO and presented to the department's DH and SDMs, and to the DAC, in order to inform them of:

- planned activities
- where roles and responsibilities lie
- the expected timeline for reporting results

The plan should be presented to the CFO and other governance bodies annually.

2. Determine the resource model

Depending on the situation, one of the following assessments of internal controls may be performed:

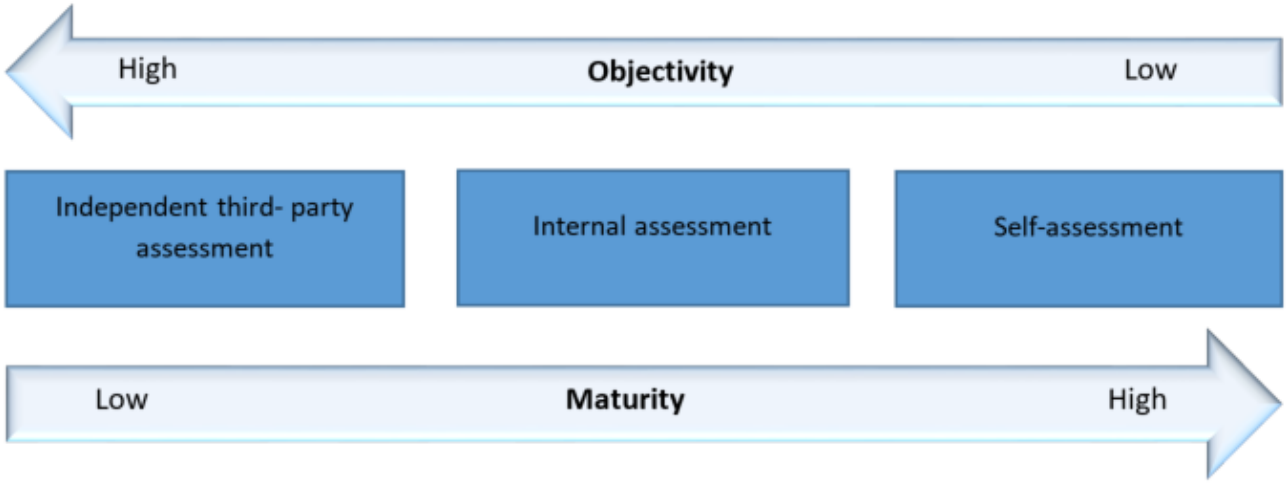
- a BPO self-assessment
- an internal assessment by a group independent from the process
- an assessment by an independent third party

The department should determine the most appropriate approach based on the following criteria:

- the available capacity
- the objectivity required
- the maturity of the program
- the risks associated with the process

Figure 3 shows the different ways that internal controls can be assessed and the degree of objectivity and maturity associated with each.

Figure 3: resource model options



▶ Figure 3 - Text version

BPO self-assessment

BPO self-assessment occurs when BPOs:

- assess their own controls
- report on the results

BPOs:

- conduct a formal review of the design and operational effectiveness of key controls
- identify potential gaps or weaknesses in controls that may need further review

A self-assessment is usually performed when:

- the process is mature and relatively stable
- the process or control is considered to be low-risk and a material weakness is unlikely
- the process was independently tested recently and no significant control gaps or weaknesses were found

Self-assessments may take the following form:

- a survey of BPOs confirms the existence of the control and obtains an assessment of it
- a BPO performs the assessment and shares the results

Independent internal assessment

An internal assessment is conducted by the department's ICT. An internal assessment is more independent than a BPO self-assessment. An internal assessments is usually undertaken when:

- the process and controls are considered higher-risk to the department's financial management
- gaps were previously identified and follow-up is needed

Data analytics may be used in internal assessment to determine whether there are potential gaps or weaknesses in internal controls. Data analytics involves reviewing transaction data to:

- reveal whether controls are working as intended
- identify potential gaps or weaknesses

Data analytics undertaken by accounting operations, contracting and procurement, or other areas of the department can help inform the need for an internal assessment. For example, a review of the data analytics of contracts under $25,000 might reveal potential contract splitting if the review finds that many contracts were issued to the same supplier for the same activity at the same time.

Third-party assessment

Assessments by independent third parties may be undertaken by one of the following:

- the department's IA function
- an independent external organization

A third-party assessment is conducted by an objective, professional entity that tests design effectiveness or operating effectiveness.

An independent third-party assessment is usually undertaken when:

- there is a higher risk associated with the process or controls
- the department does not have the technical expertise or internal resources to undertake the assessment
- there is a desire for increased objectivity and independence
- the area to be tested is sensitive and testing is best performed by an external party

3. Develop a plan

The department determines the length and content of the plan. An example of an action plan for ongoing monitoring in future years is provided in Appendix B. Additional elements related to ICFM should be included in the existing ICFR plan. The plan should provide an overview for the next 3 to 5 years, including:

- the mapping of processes to be assessed over the 3 to 5 year period, including business process controls, IT general controls and entity-level controls
- the level of testing
- the next full risk assessment

At this stage, new processes that were identified in the data-gathering phase will be incorporated into.

The ongoing monitoring plan should also include context about:

- how the plan will be delivered
- the plan's resource model, testing approach and methodology
- the plan's key roles and responsibilities

More details on these elements are provided in Appendix C.

Table 3 provides an overview of the roles and responsibilities in Step 2, using the RACI approach.

Table 3: key stakeholder responsibilities in developing the ongoing monitoring plan

Activity	Responsible	Accountable	Consulted	Informed
Determine the duration and timing of assessments	ICT	CFO	BPO, CFO and IA	CFO
Determine the resource model	ICT	CFO	CFO	CFO
Develop a plan	ICT	CFO	CFO	CFO, DAC, DH, IA and SDM

5.3 Step 3: complete the assessment

An effective ICFM system requires well-designed and operated controls. Assessing ICFM involves the following steps:

1. develop or update process documentation
2. test design effectiveness
3. test operating effectiveness
4. draw conclusions from the results and document them

1. Develop or update process documentation

Documentation typically includes a narrative, a flowchart and a control framework. For more details on each of these documents, see Appendix A.

Although a department may have documented its critical processes and controls in previous assessments, these may have changed because of:

- new legislation, regulations or policies
- a reorganization of the department's services and functions
- a move to a shared services environment
- changes to business processes
- changes to IT systems

When a financial management process is identified for assessment as part of the ongoing monitoring plan, the first step is to review the existing documentation with the BPO to identify whether changes have occurred and what updates need to be made. The documentation review may be accompanied by:

- interviews of BPOs and staff by the assessment team
- a workshop for BPOs and staff facilitated by the assessment team

Although the ICT may keep the inventory of the process documentation and the control documentation, the BPO is accountable for the accuracy of only the process documentation. Therefore, before the assessment takes place, the BPO should confirm with the ICT that both the process documentation and the control documentation are current and can be used for assessment purposes.

2. Test design effectiveness

Testing design effectiveness involves testing a control sample to see whether it effectively mitigates the risk to financial management. Such testing usually combines a walk-through and an evidence review.

In a **walk-through**, the ICT follows a transaction from start to finish (when it is recorded in the financial system) by the BPOs. A walk-through typically includes the following activities:

- enquiry with the BPO about the steps taken to complete the control
- observation of the control being performed
- examination and retention of evidence that the control was performed

In an **evidence review**, the ICT confirms that the control has performed as intended.

The objective of design effectiveness testing is to determine whether the control continues to adequately mitigate the risk. Design effectiveness testing should be conducted before operating effectiveness testing to confirm that the control is working as intended. In addition, the steps and results should be sufficiently documented so that another individual performing the same steps would arrive at the same conclusion.

3. Test operating effectiveness

Testing operating effectiveness involves assessing the control over a period of time, usually 1 year. Operating effectiveness testing assesses whether controls are operating as designed. Where not all controls have been designed effectively, operating effectiveness can be assessed for a subset of controls. To determine the operational effectiveness of a control, the assessment may include the use of:

- enquiry
- re-performance
- observation
- examination of documents

Enquiry

The assessor discusses the operation of the control with the BPO to confirm that the assessor understands:

- how the control was performed
- what information was used
- what constraints, if any, were experienced

Enquiry alone is not sufficient to draw conclusions about the operating effectiveness of the control.

Re-performance

Re-performance is typically conducted for higher-risk areas. In such cases, the assessor re-performs the control for a sample of transactions or activities to determine whether the results are consistent with those performed originally.

Observation

The assessor reviews all observable physical evidence, including observing the individual who performs the control.

Examination of documents

The assessor examines evidence that shows that the control was performed. For example, the reconciliation is saved on the network and there is evidence of review by the supervisor (sign-off or email).

The key attributes that should be tested for each control include:

- evidence that the control was conducted (for example, spreadsheet, working papers)
- evidence of review (for example, tick marks, analysis)
- evidence of approval (for example, email, sign-off)
- evidence of follow-up on issues (for example, emails)

- verification of delegation of financial authorities, as appropriate

In the event that a control failure is noted, additional testing may be used to:

- understand the extent of a potential error
- measure the impact of the control weakness

The ICT should also look for compensating controls.

The type of testing depends on the nature of the control, and volume will influence the sample size. A description of sampling is provided in Appendix D.

Table 4 provides an overview of the roles and responsibilities in Step 3, using the RACI approach.

Table 4: key stakeholder responsibilities in conducting assessments

Activity	Responsible	Accountable	Consulted	Informed
Develop or update process documentation	BPO and ICT	CFO	BPO and ICT	BPO
Test design effectiveness	BPO and ICT	CFO	BPO and ICT	BPO
Test operating effectiveness	BPO and ICT	CFO	BPO and ICT	BPO
Draw conclusions from the results and document them	BPO and ICT	CFO	BPO and ICT	BPO, DH and SDM

5.4 Step 4: capture the results and actions of the assessment

After an assessment has been completed, the ICT should:

1. report the results to the BPO
2. obtain the remediation action plan from the BPO
3. review progress against the action plan
4. report on the action plan and include the status in the Annex to the Statement of Management Responsibility Including ICFR when the controls are related to financial reporting

1. Report the results to the BPO

Following the assessment, the ICT shares the results with the BPOs. This could take the form of a table that provides:

- observations, which constitute a summary of the assessment findings

- an impact statement, which indicates the increased likelihood of a material misstatement in the departmental financial statements and the impact on resource management, achieving departmental objectives, and decision making
- recommendations, which:
    - are intended for management
    - address any control weaknesses and the issues outlined in the impact statement

It is a good practice to rank the risks in the assessment findings to make it easier for the BPO to prioritize corrective actions.

Refer to Appendix E for a sample table of recommendations.

2. Obtain the remediation action plan from the BPO

Following the assessment, BPOs should draw up a management action plan to address any gaps or weaknesses in key controls. The remediation action plan should include milestones and expected completion dates for the action items. It is a good practice to have the ICT review the management action plan to ensure that the corrective action is sufficient to address gaps and weaknesses.

The ICT obtains the management action plan from the BPO and includes it in the ICFM report.

3. Review progress against the action plan

The ICT works with the BPO to review the progress and status of remediations periodically. The ICT should:

- review progress on remediation action plans
- report on progress in the department's ICFM status reports and end-of-year report

The frequency of the review is up to the department, although twice a year is suggested. The ICT may leverage existing processes used by IA to report on management action plans.

4. Report on the action plan, including the status of the plan, in the Annex to the Statement of Management Responsibility Including ICFR

It is recommended that remediation action plans and status reports be included in the report on ICFM that is made to the CFO and the DAC. The status of remediation action plans for ICFR is indicated in the Annex to the Statement of Management Responsibility Including ICFR.

Table 5 provides an overview of the roles and responsibilities in Step 4, using the RACI approach.

Table 5: key stakeholder responsibilities in capturing assessment results and remediation actions

Activity	Responsible	Accountable	Consulted	Informed
Report the results to the BPO	ICT	CFO	BPO and SDM	BPO and SDM
Obtain the remediation action plan from BPO	ICT	CFO	BPO and SDM	BPO and SDM
Review progress against the action plan	ICT	CFO	BPO and SDM	BPO and SDM
Report on the action plan and include its status in the Annex to the Statement of Management Responsibility Including ICFR	ICT	CFO	BPO and SDM	BPO, DAC, DH, IA and SDM

5.5 Step 5: develop the internal and external reports

As noted earlier, pursuant to the *Financial Administration Act*, the DH is accountable for the effectiveness and the reporting of the department's system of ICFM. According to the *Policy on Financial Management*, the CFO and SDMs also have responsibilities for the effectiveness of ICFM. In order for the DH, CFO and SDMs to fulfill their responsibilities, they should be informed of:

- the status of the ICFM system
- any actions that are needed to address gaps or weaknesses

Such information is included in the following reports:

1. internal status reports (required for both ICFM and ICFR)
2. external reports (required for ICFR), including the Annex to the Statement of Management Responsibility Including ICFR

Under the *Directive on Internal Audit*, the DH is accountable for reporting to the DAC.

1. Internal status reports (required for both ICFM and ICFR)

Once the appropriate BPOs have completed, reviewed and validated the ongoing monitoring assessments for the year, the ICT consolidates and documents the results in a findings report. The findings report can include:

- key findings from the ongoing monitoring assessments and associated remediation action plans
- the status of any actions that have not been implemented yet

The results of the assessments should be reported to the DH, CFO, SDMs and the DAC. Reporting will vary according to a department's governance framework.

How often reports should be completed depends on the department. At least one status report should be prepared during the year, and an annual end-of-year report should be prepared to coincide with the presentation of the financial statements. If critical issues arise that could have a material impact, they should be brought to the attention of the DH, CFO and SDMs as soon as possible.

2. External reports (required for ICFR)

The *Policy on Financial Management* require that the DH and CFO sign the Statement of Management Responsibility Including ICFR. The statement prefaces the financial statements and outlines management responsibility for maintaining an effective system of ICFR. The Statement of Management Responsibility Including ICFR is supported by an annex. The annex contains a summary of the department's measures to maintain an effective system of ICFR. The annex also contains a summary of the department's ICFR assessments for the fiscal year, including progress, results and related action plans, which helpful in understanding the department's control environment.

The *Guide to Internal Control Over Financial Management* provides details on expectations for assessments of ICFR, including requirements for common service providers.

The ICT works closely with the department's financial reporting function to ensure that the Annex to the Statement of Management Responsibility Including ICFR is included in the cycle for reviewing the financial statements reporting package, which is prepared annually.

Table 6 provides an overview of the roles and responsibilities in Step 5, using the RACI approach.

Table 6: key stakeholder responsibilities for developing the internal and external reports

Activity	Responsible	Accountable	Consulted	Informed
Develop the internal and external reports	ICT	CFO	CFO, DH and SDM	CFO, DAC, DH, IA and SDM

6. References

Legislation

- *Financial Administration Act*, subsection 16.4(1)

Related policy and guidance instruments

- *Policy on Financial Management*
- *Guide to Internal Control Over Financial Management*
- *Framework for the Management of Risk*
- *Directive on Accounting Standards*(GC 1010 Financial Statements Concepts (Materiality)
- *Directive on Internal Audit*

7. Enquiries

Members of the public may contact Treasury Board of Canada Secretariat Public Enquiries if they have questions about this guide.

Individuals from departments should contact their departmentalfinancial policy group if they have questions about this guide.

Individuals from the departmental financial policy group may contactFinancial Management Enquiries for interpretation of this guide.

Appendix A: Internal control concepts

Documentation

Documentation generally includes:

- a narrative
- a flowchart
- a control framework (that includes the key risks and the controls that mitigate these risks)

Documentation should be maintainable and usable, because it will form part of the department's ongoing monitoring program. It is a good practice to validate the narrative, the flowchart and the control framework with the business process owners.

Narrative

A narrative provides:

- an overview of the process
- context for key controls

A narrative should include:

- the key stakeholders in the department that are involved in the process
- the systems used by the department

- the department-specific activities related to the process

Flowcharts and process maps

To complement the narrative, the department may choose to prepare a flowchart to show the sequence of the transactions.

Control framework

The control framework maps the key departmental controls to the control objectives and related risks. In accordance with the Committee of Sponsoring Organizations of the Treadway Commission framework, the risks to reporting include validity, accuracy and completeness. In addition to reporting risks, other risks such as timeliness could be included.

The internal control team should identify the control activities that meet the control objectives. When doing so, they should consider the following:

- more than one control may be required to fully address the risk or control objective
- a strong control activity could address more than one risk or control objective
- there should be a mix of preventive and detective controls
- automated controls are generally more reliable than manual ones

A good control:

- mitigates a risk and not just an activity or step in the process
- is formalized and standardized for consistency
- is conducted frequently and precisely enough to mitigate the risk
- is conducted by knowledgeable personnel who understand the purpose of the control

Controls in the matrix should include information on who, what, when, where, why and how. Various categories of controls are documented in the control framework and outlined below.

Categories of controls

There are 3 categories of controls:

a. entity-level controls
b. information technology (IT) general controls
c. business process controls

a) Entity-level controls

Entity-level or “tone-at-the-top” controls define an organization’s corporate culture and commitment to integrity and ethical values. They establish guidelines for an organization’s:

- governance

- financial analysis and integrity
- adherence to applicable laws and professional standards

Entity-level controls set out an organization’s values and, through policies and procedures, clarify the desired behaviour of the organizations:

- employees
- management team
- governance bodies

Entity-level controls have 5 distinct areas:

1. control environment
2. risk assessment
3. control activities
4. information and communication
5. monitoring activities

If these controls are inadequate or non-existent, their weakness or absence will fundamentally affect the reliability of controls at the process level and ultimately affect the department’s ability to achieve its objectives.

Examples of entity-level controls

- The department has developed a code of ethics that is communicated to employees via the departmental intranet (employees are required to acknowledge the code of ethics when they are hired and annually thereafter).
- The department has conducted an annual fraud risk assessment and communicates the results to the deputy head.

b) IT general controls

IT general controls help:

- ensure the reliability of financial data generated by IT systems
- support the assertion that systems operate as intended and that output is reliable

Basic IT areas that are relevant to internal controls are:

- change management
- logical security
- operations

The effectiveness of IT application or program controls depends on the effectiveness of IT general controls.

Examples of IT general controls

- The organization’s password settings meet or exceed the industry standard.

- Administrative access is restricted to individuals who need it.

c) Business process controls

Business process controls are activities carried out during the initiating, recording, processing and reporting of financial information, as well as control activities related to financial management processes. They are designed to operate at a level of precision that will prevent or detect and correct errors related to internal controls over financial management. These controls can be:

- detective or preventive
- automated or manual

Examples of business process controls

- Only budget changes that are approved by the appropriate delegated authority are entered into the departmental financial management system.
- Invoices are certified by the appropriate delegated authority before they are paid.

Appendix B: Example of action plan for future-year ongoing monitoring

Table B1 is an example of a 5-year ongoing monitoring plan. It shows regular ongoing monitoring and maintenance of a system of internal controls over financial reporting. The department determines the plan and can typically use this table to populate the portion of the annex related to action plans for subsequent years.

Table B1: example of a 5-year monitoring plan

Type of control	Risk	2019 to 2020	2020 to 2021	2021 to 2022	2022 to 2023	2023 to 2024
Entity-level control	Low	x				x
Information technology general control						
Logical security	High	x	x	x	x	x
Business process controls						
Accounts payable: invoice and payment	Medium	x		x		x
Accounts receivable: cash receipts	Low	x				x

Type of control	Risk	2019 to 2020	2020 to 2021	2021 to 2022	2022 to 2023	2023 to 2024
Contracting (procurement)	High	x	x	x	x	x
Revenue: late and erroneous filing penalties	Medium	x		x		x
Month-end and year-end accruals	High	x	x	x	x	x
Quarter-end and year-end disclosure	Medium	x		x		x
Payroll	High	x	x	x	x	x
Budgeting and forecasting	Medium	x		x		x
Revenue: base assessments	High	x	x	x	x	x
Revenue: pension plan assessments	High	x	x	x	x	x
Revenue: cost-recovered service based on memoranda of understanding	Medium	x		x		x
Revenue (other): user pay surcharges foreign office representative	Low	x				x

Appendix C: Elements of a documented ongoing monitoring plan

The following are some key elements that organizations may want to include in their documented ongoing monitoring plan. This list is not exhaustive, and departments can decide what they want to include.

Context

This section may contain a brief description of the organization’s operational environment.

Risk-assessment approach

This section may include a description of how the organization conducts its risk-based assessments, including the materiality thresholds used.

Multi-year testing plan

This plan may include a summary of control areas to be tested as a result of a risk assessment conducted over a multi-year period.

Documentation and testing strategies

This section may include a summary of the documentation methods for key control areas and a discussion of testing strategies. The strategies may include a discussion of:

- any planned testing of new processes for design effectiveness
- any redesigned processes
- the planned approach for testing the operating effectiveness of key controls

Remediation and management action plans

After testing, known control deficiencies will need to be remediated. Organizations may want to highlight how remediation and management action plans will be reported and what follow-up there will be in the management action plan.

Roles and responsibilities

This section may clarify who is responsible for what in the ongoing monitoring program for the organization. The details may include roles and responsibilities for:

- the testing of design and operating effectiveness
- the remediation of gaps in design or operating effectiveness
- the approval of the remediation methods
- the engagement of internal audit and the departmental audit committee

Reporting

This section may detail:

- how the organization reports internally and externally on the ongoing monitoring for Internal Control over Financial Reporting (ICFR) and Internal Control over Financial Management (ICFM)

- the frequency of this reporting

Appendix D: Sampling of transactions during the testing of operating effectiveness

Defining the sample population

Selecting a sample of transactions to assess is a critical step in testing operating effectiveness. The sample should reflect all the transactions or activities that comprise the process in which the control is applied.

Assessment period

It is important to:

- know the time frame for the assessment
- consider whether there have been significant changes to the control, which would affect sample selection
- recognize the risks associated with a control effectively

If a remediation action has been implemented, the control should be re-tested to confirm that it has been implemented properly. Two separate periods for assessment may be required.

Sample size

The sample should represent the transactions or activities to be assessed in order to draw conclusions about the operating effectiveness of the control. When designing a sampling plan, consider the characteristics of the items being assessed and their stratification. Things to consider include:

- whether the control is the same across regions
- whether the type of transaction results in a different method of executing the control
- any concerns that arose during previous assessment activities

The sampling practices and techniques chosen should be accurate and reliable enough to demonstrate the overall effectiveness of the control. See Table D1 for a list of industry best practices for sample size.

Frequency of control performance

The extent of testing is determined by how frequently a control is performed.

Table D1 shows industry best practices for auditors and risk practitioners to follow when selecting a sample based on which they will draw conclusions about the effectiveness of an internal control.

Table D1: industry best practices for sample size

Nature of control	Frequency of performance	Sample size
Manual	Daily	25 transactions
Manual	Weekly	10 transactions
Manual	Monthly	5 transactions
Manual	Quarterly	2 transactions
Manual	Twice yearly	2 transactions
Manual	Annually	1 transactions
Manual	As required	10% of the population or 25 (whichever is smaller)
Programmed or automated	Benchmark testing: test 1 application of each programmed activity (re-performance)	Benchmark testing: test 1 application of each programmed activity (re-performance)
Information technology (IT) general controls	Follow the guidance above for manual and programmed aspects of IT general controls	Follow the guidance above for manual and programmed aspects of IT general controls

Appendix E: Sample table of recommendations

Table E1: sample table of recommendations

Findings				
Control matrix reference	**Observation**	**Impact**	**Recommendation**	**Business owner**
Pay administration				

Findings				
Control matrix reference	**Observation**	**Impact**	**Recommendation**	**Business owner**
PRE-3A	During the review, it was noted that the pay-related action form was not approved by an appropriate delegated authority for X out 25 samples.	Without documented approval of pay-related actions, there is an increased risk of inappropriate pay-related actions.	We recommend that management enforce the requirement that all pay-related action forms be approved by the appropriate delegated authority before they are processed in the system. In addition, we recommend that a monitoring control be implemented. This control would involve performing a periodic review of pay-related action forms to ensure that approval from the appropriate delegated authority is included on each form. The review could be risk-based, in which case only a sample of higher-risk pay-related transactions would be reviewed.	Human resources
Procure to pay				
P2P-3	Based on our review of the procure-to-pay process, we noted that a user in the system is permitted to maintain vendor master files and release payments.	Not segregating the permissions to maintain vendor master files and release payments increases the risk of error or fraude.	We recommend that the department enhance segregation of permissions to ensure that individuals do not have incompatible roles in the system. We also recommend that user access be monitored periodically to ensure that access continues to be appropriate, which includes the appropriate segregation of permissions.	Procurement manager
IT general controls				

Findings				
Control matrix reference	**Observation**	**Impact**	**Recommendation**	**Business owner**
ITGC-1	During the review of change management, it was noted that, for 2 samples out of the 25 samples tested, approval from the Change Management Board was not obtained before the change was made.	Lack of approval of changes increases the risk of inappropriate changes being made to the system, which could lead to errors or create data integrity issues.	We recommend that the department follow the documented change management process and obtain the required approval. Management should also monitor changes to the system to ensure that the documented process is followed.	Not applicable

Appendix F: Definitions

accountable

In the context of the “responsible, accountable, consulted, and informed” (RACI) tables, the accountable role attests to the truth of the information or a decision that is accountable for the completion of the activity. There must be 1 accountable role for each activity.

business process owner (BPO)

For the purposes of this guide, a BPO is the individual responsible for overseeing the controls associated with a particular business process or an information technology general controls process.

chief financial officer (CFO)

A senior departmental manager who is responsible for supporting the deputy head in fulfilling their financial management responsibilities and accountabilities. More details on CFO responsibilities are outlined in the *Policy on Financial Management*, subsection 4.2.

consulted

In the context of the “responsible, accountable, consulted, and informed” (RACI) tables, the consulted role provides accurate information so that a decision can be made or an activity can be completed. There may or may not be a consulted role, and consultation may or may not be

mandatory. When consultation does occur, there is typically two-way communication between the consulted role and the responsible role.

corporate risk team (CRT)

The organization in the department that supports the deputy head with the implementation of effective risk management practices at all levels of the organization.

departmental audit committee (DAC)

A strategic resource that provides objective advice and recommendations to the deputy head about the sufficiency, adequacy, functioning and quality of the department's management, control and governance of risk frameworks and processes.

deputy head (DH)

For the purposes of this guide:

- in relation to a department named in Schedule I of the *Financial Administration Act*, its deputy minister
- in relation to any portion of the federal public administration named in Schedule IV to the *Financial Administration Act*, its chief executive officer or, if there is no chief executive officer, its statutory deputy head or, if there is neither, the person who occupies the position designated by the Governor in Council in respect of that portion

informed

In the context of the "responsible, accountable, consulted, and informed" (RACI) tables, the informed role is notified of:

- information
- a decision after it is made
- an activity after it is completed

There may or may not be an informed role. There is typically one-way communication from the responsible or accountable role to the informed role.

internal audit (IA)

A department, division, team of consultants or other group that provides independent, objective assurance and consulting services designed to add value and improve an organization's operation. IA helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluating and improving the effectiveness of governance, risk management and control processes.

internal control team (ICT)

A unit in the CFO organization that supports the establishment, monitoring and maintenance of a risk-based system of internal controls over financial management.

responsible

In the context of the "responsible, accountable, consulted, and informed" (RACI) tables, the responsible role records the information or a decision, or does the work to complete the activity by

relying on information from the consulted or accountable role.

senior departmental manager (SDM)
A departmental manager who reports directly to a deputy head and who is accountable for effective financial management in their areas of responsibility.

Footnotes

1 The RACI approach is a method of defining roles and responsibilities in a given project.

2 CRT stands for “corporate risk team.”

Date modified: 2020-05-04