Military Police Complaints Commission of Canada

Internal Controls Framework

Presented by:

Samson

Version:

December 30, 2019

Table of Contents

1. Context

Internal control is designed to assist departments and agencies in achieving their objectives. Monitoring of controls is an ongoing process to periodically assess and sustain the management of internal controls over time in support of continuous improvement.

In 2017, the Treasury Board approved a new *Policy on Financial Management*, replacing the Policy on Internal Controls (PIC). With the introduction of this new policy, the focus of internal control is on financial management.

MPCC Context

The Military Police Complaints Commission of Canada (MPCC) is a civilian, quasi-judicial oversight agency that operates at arm's length from the Government of Canada. The Commission reviews and investigates complaints concerning military police conduct and investigates allegations of interference in military police investigations. It reports its findings and makes recommendations directly to the military police and national defence leadership. As a federal institution, it is part of the Defence portfolio for reporting purposes[1].

MPCC operates under the National Defence Act[2], which provides guidance for the MPCC to conduct its investigations into complaints, the types of complaints that can be investigated and the timeframe to conduct the investigation and reporting process. The Act also provides guidance for hearings.

While the Military Police Complaints Commission of Canada has not implemented the PIC, the finance team was sensitive to the adequacy of its internal controls over many of its significant financial processes. In 2019, the CFO proposed that the MPCC adopts a more formal framework with respect to its internal controls. The proposed framework covers the internal controls over financial reporting, financial management and other key controls with respect to non-financial areas.

In the fall of 2019, MPCC undertook an environmental scan and review of its control environment in order to incorporate the necessary elements.

[1] https://www.mpcc-cppm.gc.ca/index-eng.aspx

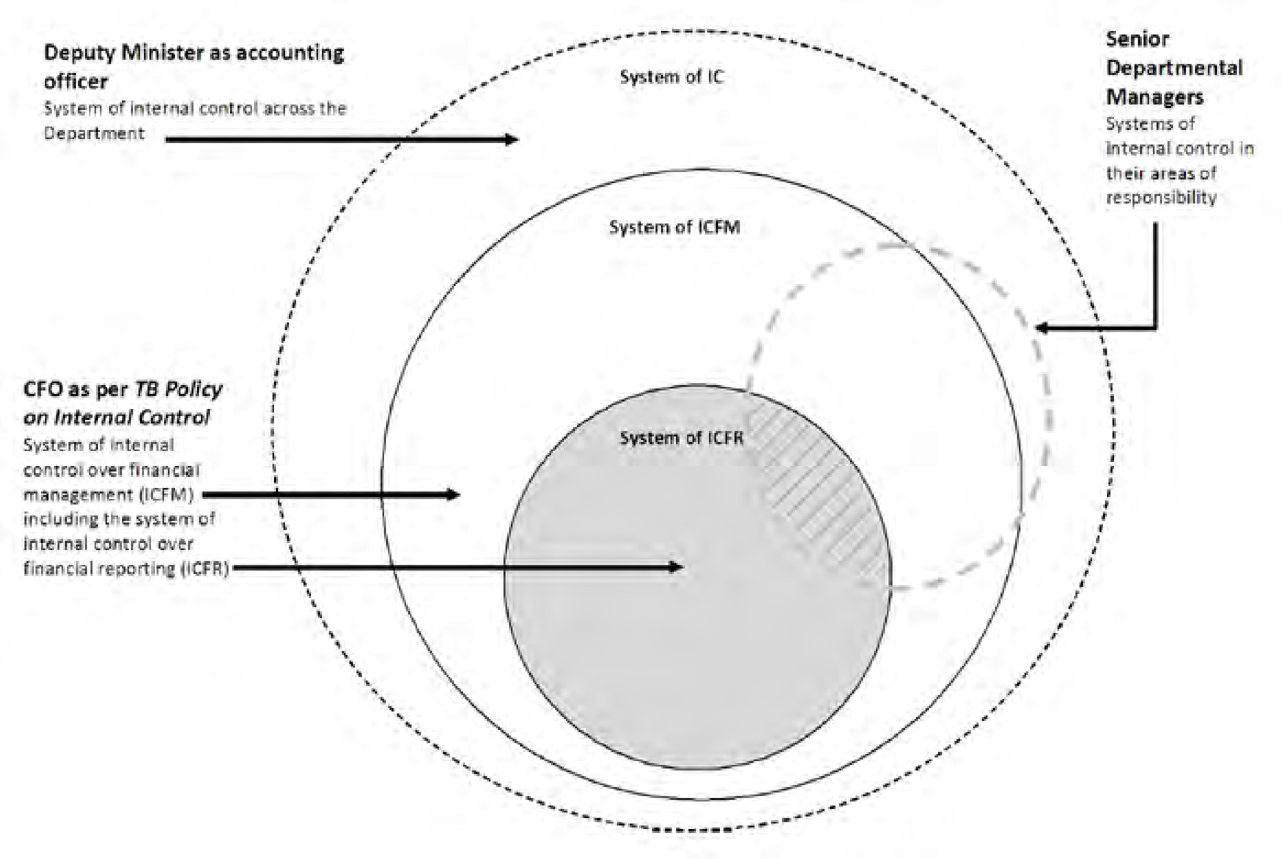
[2] https://laws-lois.justice.gc.ca/eng/acts/n-5/page-51.html#h-378808

This document is meant to provide an internal controls' framework for MPCC in the conduct of its ongoing monitoring of internal controls, taking into account the environmental scan and considerations stemming from the recent *Policy on Financial Management*. The main themes of the framework include:

- Roles and responsibilities
- ICFM environment at MPCC
- Risk assessment elements
- Five-year Monitoring Plan

2. Roles and Responsibilities

MPCC management's role in the implementation of the *Policy on Financial Management* and monitoring of its internal control system is essential to its effectiveness. As illustrated below, the deputy head, Chief Financial Officer and senior departmental managers (managers who report directly to the deputy head) all have accountabilities for the department's system of internal control.


Deputy Minister as accounting officer
System of internal control across the Department
System of IC
Senior Departmental Managers
Systems of internal control in their areas of responsibility
System of ICFM
CFO as per *TB Policy on Internal Control*
System of internal control over financial management (ICFM) including the system of internal control over financial reporting (ICFR)
System of ICFR

The following presents roles and responsibilities shared in the organization regarding the ICFM monitoring.

- **Chairperson**
  - As accounting officer and Chief Executive Officer, the Chairperson is responsible for measures taken to maintain effective systems of internal controls; and
  - Signs the *Statement of Management of Responsibility* which includes the Annex.

- **Chief Financial Officer (CFO)**
  - Leads and coordinates the establishment and execution of the annual assessment plan, and the ongoing maintenance and monitoring of an effective and integrated departmental system of ICFM and reporting; and
  - Leads and coordinates the effective and timely production of the annual *Statement of Management Responsibility Including Internal Control Over Financial Reporting*.

- **Corporate Services Branch**
  - Lead MPCC role for coordinating the ICFM assessment and ongoing monitoring; and
  - Informs internal controls assessment results and necessary changes in processes and controls.

  Note: Financial operations activities (changes) may impact the ICFM framework and the identified key controls.

- **Office of the Comptroller General**
  - Acts as lead MPCC role for internal audit (including a key source of expertise).

  Note: Internal controls assessment results can inform future internal audit plans as internal audit findings can be leveraged to support the internal control assessment

- **Managers/Business Process Owners**
  - Responsible for maintaining effective systems of internal controls in programs for which they are responsible;
  - Validate risk assessments and controls documentation for the area within their responsibility;
  - Inform Comptrollership branch of significant changes to controls and processes and provide updates to the process documentation;
  - Provide supporting documentation and other information requested to support to the team conducting the testing; and
  - Contribute to the assessment of key risks and controls in their area of responsibility.

- **IT Specialist**

  - Lead MPCC role for IT infrastructure and system applications (including a key source of expertise); and
  - Contributes to assessments of IT systems and application controls.

- **Small Department Audit Committee**
  - As part of its oversight and advisory role on internal control, the Audit Committee may wish to monitor the implementation of the *Policy on Financial Management* and as such, will provide insight on the assessment plans and results.

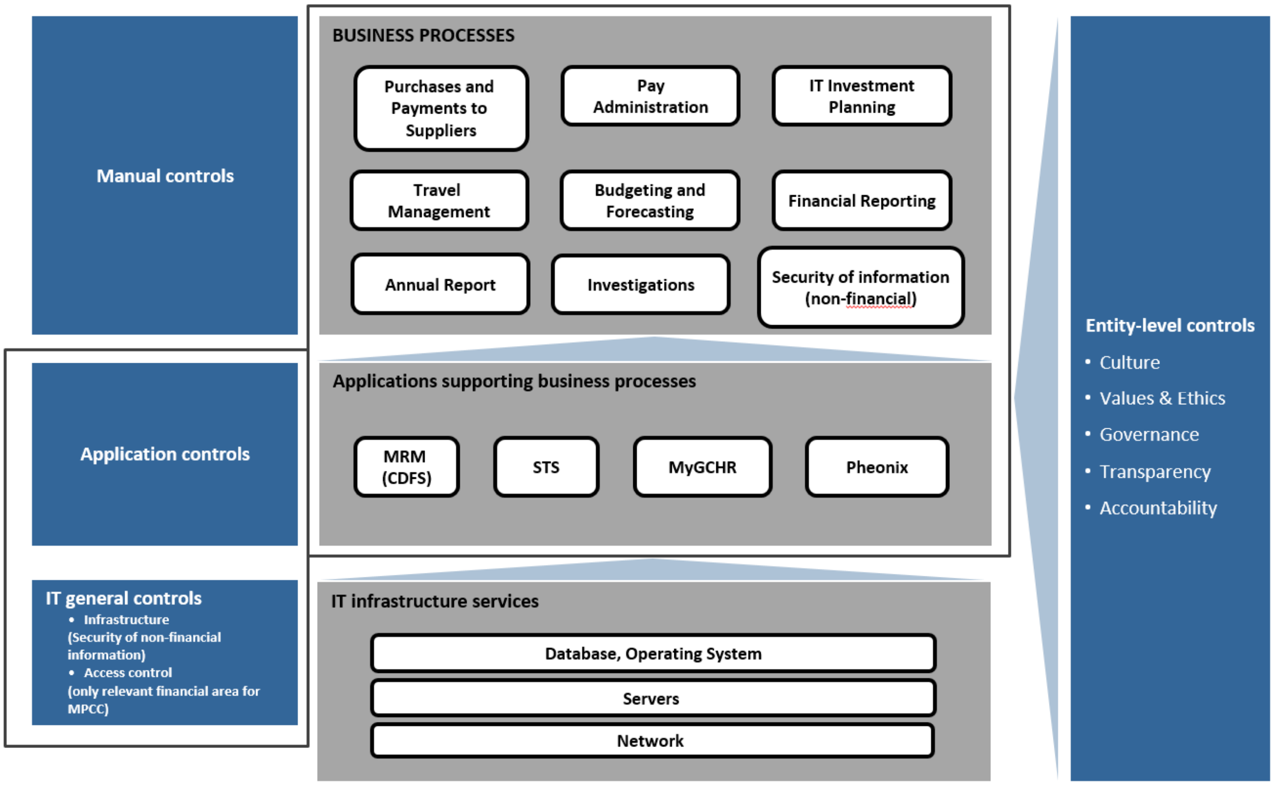
- **Other Departments and Agency Service Providers**

MPCC relies on other organizations (Common Service Providers – CSPs) for the processing of certain transactions. These CSPs must report the results of their annual risk-based assessment of the system of internal controls regarding the services they provide:

- Public Services and Procurement Canada administers the payments of salaries and the procurement of goods and services, and provides accommodation services.
- Shared Services Canada provides information technology (IT) infrastructure services in the areas of data centre and network services.
- Treasury Board of Canada Secretariat provides information related to public service insurance and centrally administers payment of the employer's share of contributions toward statutory employee benefit plans.
- MPCC's financial system related functional services are shared with the CDFS Cluster Group. The services are administered through an MOU where MPCC shares equally the expenses (including maintenance, training, user support, etc.) as well as the responsibilities and risks in relation to the financial system.
- Canadian Centre for Cyber Security (CCCS) provides cyber alerts to all departments including MPCC where the IT administrator reviews, evaluates and implements the alerts when they are applicable to the organization. This involves application updates, windows security updates, firewall site blocking and more.

3. General Principles

The internal controls environment includes a set of internal controls components as demonstrated in the diagram below:



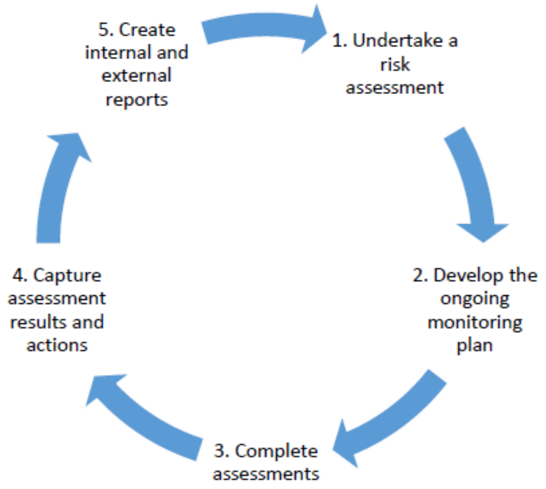
4. On-going Monitoring Approach

The proposed framework will provide MPCC with its first ongoing monitoring plan through the risk assessment update, while integrating additional financial management and program related processes.

The approach adopted by MPCC for its ongoing monitoring has been developed around the proposed guidance issued by the Treasury Board Secretariat (TBS) in October 2017[3], and includes the following five steps:

[3] Draft guidance issued by TBS in October 2017:

- *Guide on Internal Controls Over Financial Management*
- *Guide to On-Going Monitoring of Internal Controls Over Financial Management*


5. Create internal and external reports
1. Undertake a risk assessment
2. Develop the ongoing monitoring plan
3. Complete assessments
4. Capture assessment results and actions

Step 1: A detailed **risk assessment** determines areas of high risk in the department's system of ICFM that need to be reviewed as part of the risk-based approach to ICFM (conducted every five years). A more limited risk assessment, called an environmental scan, will take place in the intervening years to ensure that the plan is updated as required to reflect changes to the department.

Step 2: The **ongoing monitoring plan**, which is based on the risk assessment and an analysis of the processes and controls within the department, describes:

- The frequency of the assessments;
- The types of assessments; and
- The person who will conduct the assessments.

Step 3: The department **completes the assessments** according to the ongoing monitoring plan.

Step 4: The assessment results are **captured**, and **remediation actions** are developed.

Step 5: The assessment is then detailed in **internal and external reports** that inform and communicate the results and recommendations for remedial actions to be taken.

The approach will enable MPCC management to determine whether ICFM within the organization functions as intended (on a continuous basis), to identify internal control deficiencies, to take corrective measures to address those deficiencies and to communicate results to senior management as appropriate.

The framework includes a multi-year monitoring plan that will need to be reviewed and updated regularly. The monitoring plan is a live document and management needs to keep in mind the following fundamental questions while reviewing and updating this monitoring plan on a regular basis:

- Has MPCC identified the meaningful risks to its objectives?
- Which controls are "key controls" that will best support a conclusion regarding the effectiveness of internal control in those risk areas?
- What information will be persuasive in telling MPCC management whether the controls are continuing to operate effectively?
- Have these controls changed due to recent events?
- Is MPCC monitoring the appropriate control activities and at the appropriate frequency (e.g., every year, every 3 years)?
- Are there controls being monitored that are not key controls, if so, should they be removed from the scope?
- Are deficiencies identified and communicated in a timely manner to the responsible parties?
- Is the ongoing monitoring plan sustainable?

5. Work plan

The first step of the MPCC multi-year monitoring plan is to conduct an annual risk assessment on entity level controls, business processes, and ITGC areas to ensure that ongoing testing focuses on the highest risk areas. MPCC has adopted a model where the risk assessment is revisited in full every five years with a simpler environmental scan for the other years. This will ensure changes in risks are considered and any needed amendments to the multi-year monitoring plan are made. The decision to determine when business processes or ITGCs will be assessed is selected based on their risk rating to ensure the priority toward higher risk processes.

5.1 Entity Level and Business Process Controls

5.1.1 Risk Assessment Approach

Entity-Level Controls are controls that have a pervasive effect on an organization as they reflect the "tone at the top" and can have significant consequences on the overall assessment of the effectiveness of internal control over financial reporting. According to the COSO framework, it should cover the following elements:

- Control Environment;
- Integrity and Ethical Values;
- Risk Assessment;
- Control Activities;
- Information and Communication; and
- Monitoring.

Business Processes***:*** The following ICFM business processes, as identified by MPCC as the key processes, were considered for the risk assessment.

Key Business Process Controls	Related IT System	ICFM	Other
1. Purchase to Payments (Expenditures)	CDFS, STS	X	
2. Travel Expenditures	HRG / STS	X	
3. Pay Administration	MyGCHR	X	
4. Budgeting and Forecasting	CDFS…	X	
5. Financial Reporting and Close (financial statement close, trial balance, Treasury Board submission and financial statement reporting)	-	X	

6. IT Asset Planning	-	X	
Non-Financial Process Areas			
7. Security of non-financial information			X
8. Investigation			X
9. Annual reporting			X

5.1.2 Risk Assessment Results

Our risk assessment table includes both inherent risk and control risk, considered together to determine the overall risk ranking. More detailed risk elements supporting MPCC risk assessments are presented in Appendix A.

Process	Inherent Risk Rating	Control Risk Rating	Overall Process Risk Rating
Entity-Level Controls	**LOW**	**MEDIUM**	**MEDIUM**
Financial Management Business Processes			
– Purchase to Payments (Expenditures)	**MEDIUM**	**MEDIUM**	**MEDIUM**
– Travel Expenditures	**MEDIUM**	**MEDIUM**	**MEDIUM**
– Pay Administration	**HIGH**	**LOW**	**MEDIUM**
– Budgeting and Forecasting	**MEDIUM**	**LOW**	**MEDIUM**
– IT Asset Planning	**MEDIUM**	**MEDIUM**	**MEDIUM**
– Financial Reporting	**MEDIUM**	**LOW**	**LOW**
Non-Financial Processes			
– Security of non-financial information	**MEDIUM**	**MEDIUM**	**MEDIUM**
– Investigations	**HIGH**	**LOW**	**MEDIUM**
– Annual Report	**MEDIUM**	**LOW**	**LOW**

5.2 IT General Controls

A risk assessment was also performed over areas of ITGCs to determine the overall process risk rating for each key system relied upon. MPCC relies on Other Government Departments and Agency Service Providers who provide services including hosting services for MPCC's major IT systems. As a result, MPCC is not the business process owner of these systems and relies on third parties for the IT general controls. MPCC is, however, responsible for ensuring that user access to these systems remains appropriate and are tested as part of the business process controls listed in section 4.1.

Each ITGC area was considered in terms of the following risk factors to determine the area's overall risk rating:

- Importance / proximity to financial statements;
- Complexity of ITGC area;
- Degree of changes in underlying processes; and
- Instances of control breakdowns / gaps in the past.

Systems **(User Access Component of ITGC Only)**	**ITGC Area**	**Importance to financial management**	**Degree of change**	**Complexity / Breakdowns**	**Overall ITGC Risk Rating**
CDFS (MRM)	User Access only	High	Low	Mod	**MODERATE**
SPS	User Access only	High	Low	Low	**MODERATE**
MyGCHR	User Access only	Mod	Low	Low	**LOW**
Phoenix	User Access only	High	High	High	**HIGH**
Shared Travel Services (HRG)	User Access only	Mod	Low	Low	**LOW**

1. MULTI-YEAR MONITORING PLAN

Based on the monitoring approach presented in Appendix C, the following ongoing monitoring plan is proposed for the following five years (subject to changes based on MPCC priorities and resource levels):

		Fiscal Years					
Key Control Areas	**Risk**	**2020-21**	**2021-22**	**2022-23**	**2023-24**	**2024-25**	**Notes**
Entity-Level Controls	Medium	X					
Business Process Controls							
Purchase to Payments (Expenditures[note 1])	MEDIUM	X		X		X	Note 1
IT Asset Planning	MEDIUM		X		X		
Travel Expenditures	MEDIUM	X		X		X	
Pay Administration	MEDIUM		X		X		
Budgeting and Forecasting	MEDIUM		X		X		
Financial Reporting	LOW			X			
Non-Financial Process Areas (Suggested)							
Security of non-financial information	MEDIUM	X					
Investigations	MEDIUM		X				
Annual Report	LOW			X			
ITGC areas							
User Access (financial areas)	🟧	X		X		X	
Infrastructure (non-financial information)	🟧		X		X		

Note

1. Testing will include the payments cycle for operating and capital expenditures.

Appendix A. Risk Analysis

The risk analysis was conducted through the assessment of inherent risk and control risk:

- *Inherent Risk (IR)* is the susceptibility of an assertion to material misstatement, assuming no related controls. In other words, IR is the likelihood that a material misstatement exists in the financial statements without the consideration of internal control. The following factors were considered when assigning an inherent risk rating:

    - Size in dollars of transactions within the process;
    - Level of complexity of relevant accounting standards;
    - Extent of judgment required for process financial reporting (e.g. estimations, valuations, subjectivity required);
    - Attributes of individual transactions (e.g. homogeneity of transactions, extent of automation, volume of activity); and
    - Susceptibility to misstatement (e.g. nature of account, ability to hide failures, fraud history).

- *Control Risk (CR)* is the risk that material misstatements that could occur will not be prevented or detected by internal controls. That risk is a function of the effectiveness of the design and operation of internal control in achieving the entity's objectives relevant to preparation of the entity's financial statements. Some CR will always exist because of the inherent limitations of internal control. The following factors were considered when assigning a control risk rating:

    - Degree of change in underlying control process;
    - Instances of control breakdowns / gap in the past; and
    - Complexity of the underlying control.

The tables below illustrate our analysis of entity-level controls and business process controls. The combined or overall risk rating will determine the extent and frequency of testing.

A.1. Entity-Level Controls

Process	Materiality	Policy changes	judgment required	Attributes of transactions	Susceptibility misstatement	Inherent Risk Rating	Degree of change	Instances of control breakdowns	Decentralized Environment	Complexity of control	Control Risk Rating	Overall Process Risk Rating
Entity Levels	LOW	LOW	LOW	LOW	LOW	**LOW**	LOW	MEDIUM	HIGH	MEDIUM	**MEDIUM**	**MEDIUM**

A.2 Key Business Process Controls

Process	Materiality	Changes	judgment required	Attributes of transactions	Susceptibility errors	Inherent Risk Rating	Degree of change	State of Controls	Decentralized Environment	Complexity of control	Control Risk Rating	Overall Process Risk Rating
Financial Management Process Areas												
Purchase to Payments (Expenditures)	HIGH	LOW	MEDIUM	HIGH	MEDIUM	**MEDIUM**	LOW	MEDIUM	LOW	MEDIUM	**MEDIUM**	**MEDIUM**
Travel Expenditures	MEDIUM	LOW	MEDIUM	MEDIUM	MEDIUM	**MEDIUM**	LOW	MEDIUM	LOW	MEDIUM	**MEDIUM**	**MEDIUM**
Pay Administration	HIGH	HIGH	MEDIUM	HIGH	HIGH	**HIGH**	LOW	MEDIUM	LOW	LOW	**LOW**	**MEDIUM**
IT Asset Planning	HIGH	MEDIUM	MEDIUM	MEDIUM	MEDIUM	**MEDIUM**	MEDIUM	MEDIUM	LOW	MEDIUM	**MEDIUM**	**MEDIUM**
Budgeting and Forecasting	HIGH	MEDIUM	HIGH	LOW	LOW	**MEDIUM**	LOW	HIGH	LOW	LOW	**LOW**	**MEDIUM**

Process	Materiality	Changes	judgment required	Attributes of transactions	Susceptibility errors	**Inherent Risk Rating**	Degree of change	State of Controls	Decentralized Environment	Complexity of control	**Control Risk Rating**	**Overall Process Risk Rating**
Financial Reporting and Close	HIGH	LOW	MEDIUM	LOW	LOW	**MEDIUM**	LOW	LOW	LOW	LOW	**LOW**	**LOW**
Non-Financial Process Areas												
IT Security of Non-financial information	HIGH	HIGH	MEDIUM	LOW	MEDIUM	**MEDIUM**	MEDIUM	MEDIUM	LOW	HIGH	**MEDIUM**	**MEDIUM**
Investigations	HIGH	MEDIUM	HIGH	HIGH	MEDIUM	**HIGH**	LOW	LOW	LOW	HIGH	**LOW**	**MEDIUM**
Annual Report	MEDIUM	LOW	MEDIUM	MEDIUM	LOW	**MEDIUM**	LOW	LOW	LOW	MEDIUM	**LOW**	**LOW**

Appendix B. Ongoing Monitoring Approach

There are three key steps in the monitoring of activities:

1. Completing the Assessments (Testing)
2. Capturing Assessment Results and Actions
3. Reporting on Assessment Results

Note – It is recommended to conduct a walkthrough of each key process every year to confirm process flow and controls. This may not always be possible based on allocated resources.

5.1 COMPLETING THE ASSESSMENT

The multi-year monitoring plan can build upon the documentation, testing methodologies, sampling strategies, etc. developed from the design effectiveness and operating effectiveness stages of the previous ICFR roadmap. As such, the assessment for previously identified (and assessed) business processes will involve:

- An update of the process documentation, key controls and control matrix;
- The conduct of design effectiveness testing (walkthrough); and
- The conduct of operating effectiveness testing (actual testing of controls).

For new business processes, MPCC will need to:

- Document the process, identify the key controls and prepare a control matrix;
- Conduct design effectiveness testing (walkthrough); and
- Conduct operating effectiveness testing (actual testing of controls).

The nature, extent and frequency of control testing is linked to the risk level associated with the processes and/or the systems in place. The following sections will provide guidance on the level of testing required.

5.1.1 Nature of Testing

TYPE OF ACTIVITIES	PROCESSES DOCUMENTATION	DESIGN EFFECTIVENESS	OPERATING EFFECTIVENESS
DEFINITION	Support the assessments of design and operating effectiveness at all levels Key controls need to be appropriately documented.	Refers to whether controls are properly designed to achieve control objectives if they operate as defined.	Refers to whether controls consistently operate as designed.
HOW	Development or update of **process narratives**, process flowcharts, and risk and control matrices.	**Walkthrough** to confirm flow of information to get an understanding of the operation of controls.	**Testing** a sample of transactions to determine whether internal controls are operating effectively over the period.
FREQUENCY	Annually	As necessary (following a remediation measure, a change/new process, controls or new risk identified).	Operating effectiveness testing is performed once successful design effectiveness testing has occurred. Multi-year rotational based on risk: **HIGH**: Annually **MEDIUM:** Every 2 years **LOW:** Every 3 years
SAMPLE SIZE	All processes	One transaction	See Sampling Table

1.1.2 Sampling for Testing Operating Effectiveness

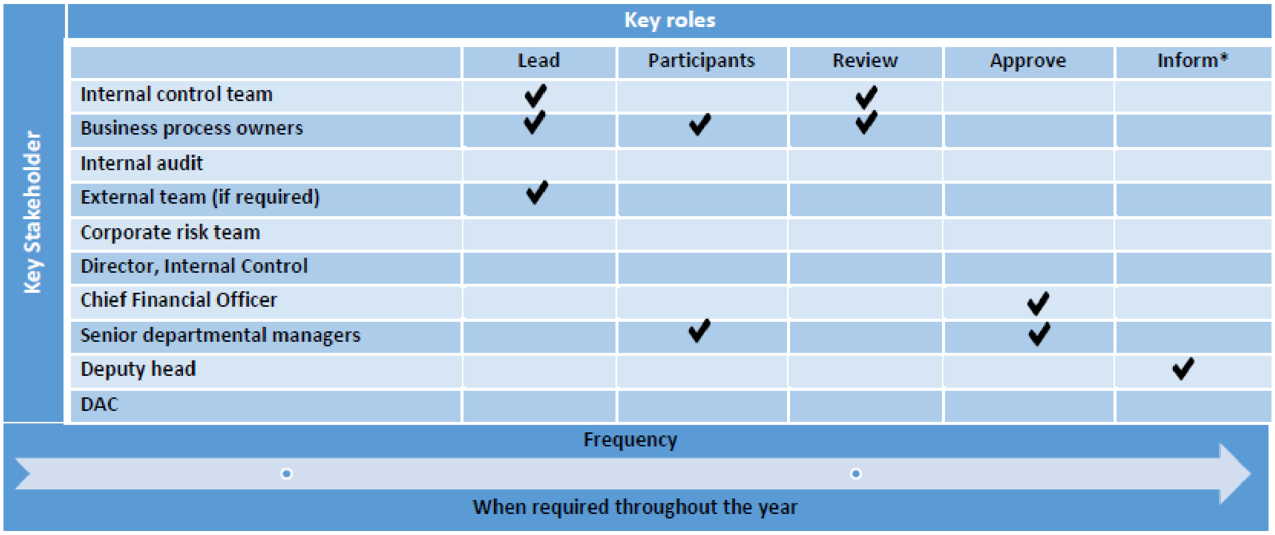
The table below is based on widely recognized statistical theory and principles.

Nature of Control	Frequency of Operation	Range for Sample Size	
		With Lower Risk of Key Control Failure	With Higher Risk of Key Control Failure
Manual	Many times a day	25	40
Manual	Daily	15	25
Manual	Weekly	5	8
Manual	Monthly	2	3

Manual	Quarterly	1	1
Manual	Annually	1	1
Automated	Test of one for each automated control activity		

Following the testing, it is essential to complete the documentation of the testing results and analyze the testing results and the need of remediation, as necessary. It is also important to brief and validate the overall testing results and action plans with the process owners/business partners.

The following table provides an overview of the key stakeholders and their responsibilities on this important step:



	Key roles				
Key Stakeholder	Lead	Participants	Review	Approve	Inform*
Internal control team	✓		✓		
Business process owners	✓	✓	✓		
Internal audit					
External team (if required)	✓				
Corporate risk team					
Director, Internal Control					
Chief Financial Officer				✓	
Senior departmental managers		✓		✓	
Deputy head					✓
DAC					

Frequency

When required throughout the year

5.2 Capturing Assessment Results

Following the assessment step, the Internal control team should document the agreed upon remediation action plan, review and track its progress, and report on it annually.

5.3 Reporting on Results

5.3.1 Internal Reporting

Once the appropriate business owners have completed, reviewed and validated ICFM ongoing monitoring assessments for the year, the results are consolidated and documented in a findings report by the Internal control team. The report will include:

- Key findings from the ongoing monitoring assessments and associated remediation action plans; and
- The status of the implementation of the remediation action plans, specifically, outstanding actions that have not been implemented.

The results of the assessments will be reported to key stakeholders annually including the Chairperson, the CFO, senior departmental managers and the DAC.

5.3.2 External Reporting

Statement of Management Responsibility Internal Control over Financial Reporting

The Policy requires that the Chief Executive Officer sign-off annually on the "Statement of Management Responsibility Including Internal Controls over Financial Reporting". This statement includes an acknowledgement of Management's responsibility for maintaining an effective system of internal control and that an assessment for the year ended was completed and that an action plan was prepared.

Annex to Statement of Management Responsibility

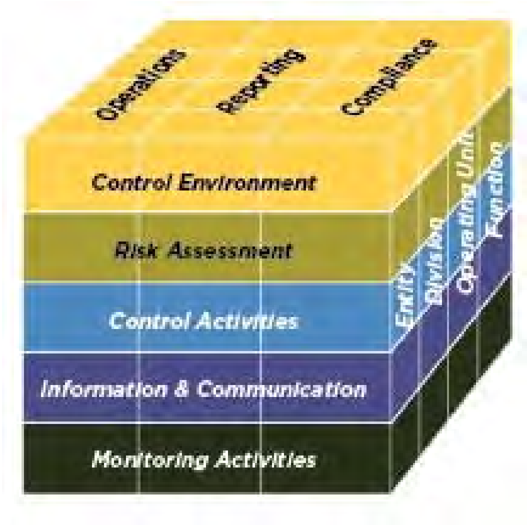
An overview of the results and action plans of the MPCC's annual assessment of the effectiveness of the system of ICFR are to be provided in an annex to the Statement of Management Responsibility. A sample annex and Statement of Management Responsibility have been provided in the draft *Guide on Internal Control over Financial Management* issued by TBS in October 2017.

The list of ICFM related processes is somewhat different than the ICFR list presented in the Statement of Management Responsibility over ICFR and the related annex. The external reporting requirement focus on ICFR has terminology associated with financial statement line items while ICFM focuses on management processes. We have proposed a reconciliation between ICFM key processes and ICFR processes reported by the Agency. Appendix B presents this reconciliation.

APPENIX B ALIGNMENT WITH COSO FRAMEWORK

In performing its assessment of Internal Controls over Financial Management, MPCC may choose to select a framework such as the 2013 COSO Framework as its applicable internal control framework, which is in-line with other federal departments and agencies.

In 1992, The Committee of Sponsoring Organizations of the Treadway Commission (COSO) developed its Enterprise Risk Management — Integrated Framework which is often referred to as the "COSO Framework".



The COSO Framework states that "Internal control" is a process, affected by an entity's directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations;
- Reliability of financial reporting; and
- Compliance with applicable laws and regulations.

When performing its risk assessment, MPCC needs to ensure that these objectives are addressed. For example, the key business process controls identified during the risk assessment are aligned with the following objectives:

Business Processes Controls	Operations	Reporting	Compliance
Payments (Expenditures)	X		X
IT Asset Planning	X	X	
Travel Expenditures	X		X

Business Processes Controls	Operations	Reporting	Compliance
Pay Administration	X		X
Budgeting and Forecasting	X	X	
Financial Reporting		X	X
Security of non-financial information	X		X
Investigations	X		X

As demonstrated above, there is significant overlap between the three main objective categories, which demonstrates the importance of the business process controls identified. This includes insuring that both financial and non-financial information is safeguarded, loss through waste, inefficiency or poor business decisions of MPCC's assets are prevented and that activities are conducted in accordance with applicable laws and regulations.

There are five interrelated components of internal control. Four components relate to the design and operation of the system of internal control:

- Control environment;
- Risk assessment;
- Control activities;
- Information and communication; and
- Monitoring activities.

These components are the basis and foundation for the testing of entity level controls.