Military Police Complaints Commission

Internal Controls Monitoring – 2021/22

Final Report

Presented by:

Samson

Version:

December 31 2021

Table of Contents

EXECUTIVE SUMMARY

Since 2017, the Military Police Complaints Commission (MPCC) has developed process controls over financial reporting and is in a mature phase of the implementation of the Policy on Internal Control.

The scope of work therefore included the following:

- Entity Level Controls
- Procure to Payment
- Travel Expenditures
- User Access
- Security of non-financial information

Entity Level Controls

The assessment found that key entity level controls over financial reporting were effective for the most part, some areas for improvement were however noted.

Business Process Controls

The assessment found that key internal controls over financial reporting related to the business processes in scope for the year 2021-22 were effective for the most part, some areas for improvement were however noted.

User Access

We consider that the user access controls related to MPCC' systems in scope are appropriate. We have noted some areas for improvements.

1. Introduction

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. As a result, the Military Police Complaints Commission of Canada (MPCC or Commission) took the initiative to document significant business processes and controls. The Commission carried out the assessment of the design effectiveness and operating effectiveness of its internal controls and put in place adequate Management action plans to address the opportunities for improvement identified.

The 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.

During fiscal year 2019/20, the Commission prepared an Ongoing Monitoring Plan for its internal controls in order to provide senior management assurance over their continued effectiveness. The ongoing monitoring of MPCC's internal controls provides assurance to client Departments that financial controls over MPCC services are effective, in support of the signature of the Statement of Management Responsibility Including Internal Control over Financial Reporting, in compliance with the Policy on Financial Management.

The following business processes were considered significant and are part of the Ongoing Monitoring Plan:

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
ITGCs Areas			
10. User Access (financial areas)	CDFS, Phoenix, STS, HRG		X
11. Infrastructure (non-financial information)			X

2. Objective and Scope

Samson & Associates was engaged to conduct documentation review, walkthroughs and effectiveness testing for the elements in scope as part of the Ongoing Monitoring Plan for the year 2021-22 (See Appendix A).

2.1 Documentation

Documented the key processes and controls in place in the form of a business process narrative, process map and control matrix and ensured they represent the current processes and controls in place.

2.2 Walkthrough and Testing

Conducted a walkthrough and performed the design and operating effectiveness testing for the following processes for MPCC:

- Entity-Level Controls
- Procure to Payment
- Travel Expenditures
- User Access
- Security of non-financial information
  (Preliminary testing only – full testing will be conducted in 2022/23 with the investigation process)

The following methodology was used over the course of the engagement:

1. Identify the key controls that should be tested
2. Elaborate testing strategy (including sampling)
3. Obtain populations and select samples
4. Conduct walkthrough
5. Assess Design Effectiveness
6. Conduct Operating Effectiveness
7. Conclude on testing

The sampling methodology used for a sample selected was based on the approach adopted by Treasury Board in their Guide to Ongoing Monitoring of Internal Controls Over Financial Management. The extent of testing was determined by how frequently a control is performed.

3. Entity Level Controls

There are five interrelated components of internal control. Four components relate to the design and operation of the system of internal control. These components are the basis and foundation for the testing of entity level controls. Our review of documentation and interviews found that ELC at MPCC were satisfactory in most cases:

Entity Level Control Elements	Assessment
Control Environment	Effective
Risk Assessment	Opportunity for Improvement
Control Activities and Related Monitoring	Effective
Information and Communication	Effective

3.1 Control Environment

Whether through its guidance and multi-layered management structures that promotes appropriate responsibilities in the pursuit of its objectives, MPCC demonstrates a commitment to integrity and ethical values. MPCC has also adopted good management practices, for example: establishment of an Executive Committee, business planning and monitoring, formal employee communication and oversight activities. MPCC's Executive Committee is kept apprised on activities and investigations being conducted in the organization. Weekly highlights are presented to them and discussed as required. MPCC has undertaken some activities for succession planning by assessing its workforce, MPCC would benefit from continuing its succession planning activities by identifying key positions and individuals who would be in the position to succeed.

Furthermore, MPCC has engaged with Health Canada to establish an Interdepartmental Letter of Agreement on Employee Assistance Services – Alternative Dispute Resolution Services. This provides MPCC with ombuds and informal conflict management services as well as access to HC's Harassment and Violence Unit. The Public Service Employee Survey is completed by a high number of employees at MPCC and the results have shown that overall employees are satisfied with the work place.

3.2 Risk Assessment

Risk assessment involves identifying and analyzing risks (both internal and external) relevant to achieving business objectives, including those related to financial management. As part of our review, we were expecting MPCC to have a process for the identification, analysis, and management of risks relevant to its activities. MPCC has a risk management function that has been working on the entity's Departmental Plan and has conducted risk assessments to identify key areas such as security and information. As part of our review, we noted however, that while a threat assessment was conducted, MPCC would benefit from expanding their assessment to include the risk of fraud for the organization as a whole. As a result, MPCC should consider expanding their current protocol for reporting wrongdoing to explicitly include the risk of fraud. Furthermore, with the including of fraud risk assessments, awareness of identifying and reporting fraud should be included in the communications on disclosure of wrongdoing to all staff.

> **Recommendation 1:** We recommend that MPCC enhance their threat assessment to include the risk of fraud and ensure that employees are aware of the risk of fraud, how to identify it and reporting protocols.

3.3 Control Activities and Related Monitoring

Control activities are the actions established by policies and procedures to help ensure that management directives to mitigate risks are carried out. Control activities are performed at all levels of the entity and at various stages within business processes, and over the technology environment. They may be preventative or detective in nature and may encompass a range of manual and automated activities.

Related to the control activities is the monitoring of the quality of the entity's internal control performance over time. Effective monitoring is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

Since 2019, MPCC has adopted a rigorous control framework and on-going monitoring plan for internal controls over financial reporting. As a result, the control activities and related monitoring are considered adequate and sufficient. An internal control follow-up process to ensure that recommendations are addressed and implemented will be implemented in 2022.

3.4 Information and Communication

The objective of this ELC element is to ensure that pertinent information is identified, captured, and communicated in a form and timeframe that enables people to carry out their responsibilities. Information systems produce reports containing operational, financial, and compliance-related information that make it possible to run and control the business. Effective communication must also occur in a broader sense i.e. Individuals must understand their own role in the internal control system, as well as how individual activities relate to the work of others. Individuals must have a means of communicating significant information upwards within the organization.

As indicated previously (section 3.1), MPCC has adopted several practices that have helped document and communicate necessary information throughout the organization. While MPCC is not a large organization, it has adopted many mature practices. The recommendation 1 made previously will further help improve how key information is communicated.

4. Results – Business Processes

Key Financial Processes	Design / Operating Effectiveness	Key Control Deficiencies	Number of Key Controls
Purchase to Payments	Opportunities for improvement	2	11
Travel Expenditures	Opportunities for improvement	2	8
Security of Non-Financial Information*	Opportunities for improvement	-	-

*Most of the Non-Financial Information that requires security protocols relates to investigations. This Investigation process will be assessed in 2022/23 and it is intended that detailed operating testing be conducted at that time. Samson focused on the design effectiveness testing in 2021/22.

In 2021/22, we focused on the design effectiveness and obtaining a proper understanding of the information management system user access and documentation management protocols (Documentum).

4.1 Procure to Payment

The scope of the controls for the Procure to Payment business process starts with completing a MPCC local purchase form. The form is sent to FAA S.32 for approval and the commitment is recorded in CDFS. To ensure that commitments are maintained and updated in a timely manner, MPCC maintains a tracking spreadsheet for all commitments recorded. This spreadsheet is updated when invoices are received and recorded against commitments. It was noted that in 2 out of 15 instances, the spreadsheet wasn't updated.

> **Recommendation 2:** We recommend that MPCC ensures that commitments are updated when invoices are received to ensure the accuracy of unencumbered funds and that unused funds are released.

A contract or purchase order is created for the purchase. After the goods have been received or the services rendered, invoices are received in the Finance inbox and sent to the appropriate delegated authority who performed a review of the invoice and certifies pursuant to FAA S.34. Then the invoice is sent back to Finance Services for payment. When the invoice is received by Finance Services, quality assurance is performed to ensure the payment is appropriate in support of FAA S.33. Once the payment has been approved it is released through SPS.

When needed, changes made to the vendor master file are received from the supplier. The request is received and verified by the Procurement Officer or the Financial Clerk who enters the change in CDFS through the security ZZZZ access. All changes input are reviewed and approved by the FAA S.33 Finance Officer.
During our testing, it was noted that access to add or remove vendors from the vendor master file is granted to all users in Finance Services. Therefore, there is no segregation of duties between users who have access to add/remove vendors from the vendor master file and access to process accounts payable. There are compensating controls in place, given that MPCC is a very small organization, where changes made to the vendor master file done by two individuals.

Excessive access to the systems increases the risk of segregation of duties where individuals have access to multiple functions in CDFS.

> **Recommendation 3:** We recommend that monitoring controls be put in place to ensure that the segregation of duty risk identified can be managed. Possible system notifications could be put in place to manage the risk.

4.2 Travel

The scope of the controls for the Travel expenditures business process starts with identifying the need to travel, approving travel requests pursuant to Expenditure Initiation Authority and FAA S.32, certifying travel claims pursuant to FAA S.34 and processing the claims for payment pursuant to FAA S.33.

A travel request is created by a travel arranger on behalf of the traveler using the online booking tool in STS. The request is routed to the appropriate delegated authority pursuant to FAA S.32 for approval and the employee can proceed to make travel arrangements once approval has been obtained. Once the travel is complete, the traveler provides all the receipts collected during travel to the travel arranger. The Travel Arranger then creates a travel claim with all the receipts attached as supporting documentation. the travel claim is routed to the delegated authority for approval pursuant to FAA S.34. The travel arranger selects the approver for the travel request and travel claim from a dropdown menu in STS. Afterwards, the claim is routed to the Processor who performs quality assurance on the claim before approving the payment pursuant to FAA S.33. Once the payment has been approved it is released through SPS.

During our testing of user access in STS it was noted that individuals had access to functions that were not required per their job duties, as follows:

- 5 out 9 users should no longer have access to approve travel requests pursuant to FAA S.32 in STS; and,
- 5 out 9 users should no longer have access to approve travel claims pursuant to FAA S.34 in STS.

Inappropriate access increases the risk of unauthorized access to STS, which could lead to accidental or intentional corruption of data; thereby, putting the integrity of corporate information at risk.

> **Recommendation 4:** We recommend that, on an ongoing basis, logical access to STS be removed immediately upon an employee leaving the Commission or an employee changing roles and no longer requiring access per their job duties. Furthermore, we recommend that there be a periodic review of access to detect any anomalies and correct them in a timely basis.

4.2 Security of Non-Financial Information

As indicated previously, the individual file testing to assess the appropriate security handling of investigation files will be assessed as part of the investigation process in 2022/23. In. 2021/22, we focused on the design effectiveness (understanding the control environment and approach) for other documentation.

Following the COVID-19 outbreak that forced the MPCC staff to work remotely, the organization has adopted a virtual approach. This was done using the existing systems (Documentum and Shared Drive) and the recent adoption of Office 365.

We have reviewed the documentation on hand by MPCC and aside from the investigation files, there is very little secured information that is being managed on its corporate systems.

Corporate documentation management practices are done using the Documentum platform and clear documentation and user access standards exists. However, the shared drive and Teams do not have the same level of document management controls.

At the time of our assessment, not all the physical files had been transferred digitally in an easily accessible manner on the shared drive, Teams or Documentum. MPCC needs to adopt a QA process to ensure that the file digitization is complete and accurate.

> **Recommendation 5:** We recommend that information management practices and protocols be but in place for all electronic information management systems, whether through Documentum, the shared drive or Teams.
>
> **Recommendation 6:** We recommend MPCC adopts a QA process for its digitization initiative to ensure that key physical records get digitize in a fashion that the document integrity is maintained.

CONCLUSON ON BUSINESS PROCESS CONTROLS

The assessment found that key internal controls over the business processes were generally operating effectively.

5. RESULTS ITGC's

2021-22	CONTROL AREAS	COMMON CONTROLS	CDFS	MYGCHR (L&O)	DOCUMENTUM	SPS (SUPPLIERS)	HRG (TRAVEL)
IT Management	3	Out of scope in 2021-22					
IT Security (User Access)	6	Opportunity for improvement	Strong	Strong	Strong	Strong	Strong
Application development and change management	4	Out of scope in 2021-22					
Computer and network operations	1	Out of scope in 2021-22					

Note: Appendix B

5.1 User Access Controls: Arrival and Departure

The key user access controls are performed when employees arrive within an organization and when they leave. It is upon arrival that majority of the user access assigned, approved, and implemented and upon departure that necessary measures are taken to remove these accesses. 12 user access were tested as part of our assessment. At MPCC, a form is used it both cases to document these steps. While a documented process was not necessarily in place more than 5 years ago, it has been in place for over two years.

We have found the arrival controls to be effective. The few employees where a documented arrival form was not available had been within MPCC for many years and their user accesses were appropriate.

However, we found employees that had left MPCC but for which systems accounts remained active:

- Five users for HRG
- Two users for CDFS

We were not able to confirm if the network access to these employees had been removed in a timely manner, but they no longer had network access at the time of our audit work.

While user access is important, we are not aware of any misuse of system access by these employees and in most cases, the risk related to the specific application is limited due to a necessary network access (which appeared to have been removed). It must be noted that the MPCC departure process requires a number of manual interventions in order to inform the appropriate individuals to remove the accesses in a timely fashion.

> **Recommendation 7:** We recommend that the departure process be formalized to ensure a timely removal of all application and network access upon departure. Documentation should be available to demonstrate when the user access have been removed (applications and network access).

5.2 On-going User Access Review

A business owner has been identified for each system within the organization. In addition to the approval of user access at the time of hire for each employee (contractor), a regular review of user access should be performed to ensure that accesses are still necessary and appropriate.

While an annual periodic and documented review of accesses appears in place for most application (compensatory controls), we have not found documentation for the network access review.

> **Recommendation 8:** We recommend that the on-going review of user access be documented for future reference.

CONCLUSION ON USER ACCESS CONTROLS

We consider that the user access controls for the systems in scope are generally appropriate.

Appendix A : On-going Monitoring Plan :

Key Control Areas	Risk	Fiscal Years					Notes
		2020-21	2021-22	2022-23	2023-24	2024-25	
Entity-Level Controls	Medium	x					
Business Process Controls							
Purchase to Payments (Expenditures[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							
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		

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

Recommendations	Risk Rating	Management Action Plan
Entity Level Controls		
Recommendation 1: We recommend that MPCC enhance their threat assessment to include the risk of fraud and ensure that employees are aware of the risk of fraud, how to identify it and reporting protocols.	**Medium**	The MPCC will integrate the risk of fraud to their next cyclical threat and risk assessment in 2025 or if the MPCC office space has a significant change prior to that date. In the meantime, the MPCC will update their security awareness communication plan, more specifically the article in the month of March on Fraud Prevention Month to incorporate information on who employees should communicate with if they encounter fraud while working and how to identify it.
Business Process Controls		
Recommendation 2: We recommend that MPCC ensures that commitments are updated when invoices are received to ensure the accuracy of unencumbered funds and that unused funds are released.	**Low**	The Finance Team will put in place standard operating procedures to ensure that commitments are kept up to date, both in our commitment spreadsheet and in CDFS. The procedures will clarify the timing and individuals/positions responsible for entering, reviewing and approving the information. In addition, we will perform semi-annual reviews of the commitments to ensure accuracy and completeness. We plan on implementing this process in time for the start of fiscal year 2022-23.
Recommendation 3: We recommend that monitoring controls be put in place to ensure that the segregation of duty risk identified can be managed. Possible system notifications could be put in place to manage the risk.	**Medium**	The MPCC will address the segregation of duty risk by revisiting our CDFS accesses and seek CDFS HelpDesk guidance in limiting the access surrounding vendor/supplier change. A preferred option is to separate the “create” and “approve” accesses between Section 33 approvers (approve only) and the other finance users (create/modify only). The change request has been submitted to CDFS with a proposed timeline of 6 months (September 2022).
Recommendation 4: We recommend that, on an ongoing basis, logical access to STS be removed immediately upon an employee leaving the Commission or an employee changing roles and no longer requiring	**Medium**	HR will now send a termination email to the finance inbox when an employee leaves the MPCC. This will then trigger the travel coordinator to suspend the accounts in the travel portal. We also recommend that

Recommendations	Risk Rating	Management Action Plan
access per their job duties. Furthermore, we recommend that there be a periodic review of access to detect any anomalies and correct them on a timely basis.		at the end of each fiscal year, HR sends a report of all terminated employees from that fiscal year, and the coordinator will then proceed with a review to make sure no employees were missed.
Recommendation 5: We recommend that information management practices and protocols be but in place for all electronic information management systems, whether through Documentum, the shared drive or Teams.	**Medium**	The MPCC currently has documented information practices and protocols for its departmental information system, Documentum. The MPCC is working on documenting document management and retention on the Microsoft Teams platform and will be implementing a policy, protocol and forms in fiscal year 2022-23. As the MPCC is currently working to retire shared drives, the management of this information will be addressed through the retirement of shared drive by the end of Fiscal year 2023-24.
Recommendation 6: We recommend MPCC adopts a QA process for its digitization initiative to ensure that key physical records get digitize in a fashion that the document integrity is maintained.	**Low**	In 2017, the MPCC adopted and documented a quality assurance process for its digitization initiative to ensure that physical records are digitized in a manner that ensures document integrity. However, there are concerns that the process was not followed properly in the past and some physical records are currently being kept as a back up to digitized records. The MPCC will put in place a plan by the end of 2022-23 to perform the quality assurance process of physical records that were digitized in a manner that ensures document integrity and to proceed to the timely disposition as per the Data Disposition Policy. In addition, the MPCC is in the process of approving a revised version of the Information and Data Disposition Policy. Once approved, the MPCC, through its legal services and over the next year, will carry out an audit before destruction of the files already digitized in order to identify the key documents which must be kept for consultation later.
User Access		

Recommendations	Risk Rating	Management Action Plan
Recommendation 7: We recommend that the departure process be formalized to ensure a timely removal of all application and network access upon departure. Documentation should be available to demonstrate when the user access have been removed (applications and network access).	**Medium**	The MPCC shall modify its departure forms to include additional fields in regard to IT related accesses to ensure those accesses are removed upon the departure of employees. For specific accesses within the Finance team, a separate document to track these accesses will be created to track modifications and deactivation as required.
Recommendation 8: We recommend that the on-going review of user access be documented for future reference.	**Low**	The MPCC is in the final stage of a new IT Security Policy which includes new measures for the control of accesses. The policy will formalize roles and responsibilities between IT and managers in the attribution of access and notifications when changes in employment or access profiles occur. The policy will also require record keeping of access changes through standardized procedures and forms.