

Compliance and Monitoring Annual Progress Report

Fiscal 2023

Prepared for Comptroller General
June 2023

Contents

- Summary of Compliance and Monitoring Activities 4**
- Mass Payment Monitoring..... 6**
 - Scope and Approach 6
 - Monitoring Outcomes 7
- Compliance and Monitoring Activities..... 8**
 - Scope and Approach 8
 - Predictive Analytics Results 9
 - Document Review Results 9
 - Event Driven Reporting 10
 - CFO Alerts 12
 - Expanding Compliance Coverage..... 12
 - Internal Control Framework..... 13
- Forensic Accounting Services..... 14**
 - Background and Objectives 14
 - Financial Risks Reported 14
 - Fraud Awareness Initiatives 15
 - Fraud Risk Management Framework..... 16
- Appendix A: Compliance and Monitoring Initiatives Update 17**
- Appendix B: Fraud Risk Management Framework Assessment..... 19**

What is in this Report

This report is a summary of Corporate Compliance and Controls Monitoring Branch (3CMB) activities and outcomes for fiscal year 2023.

What Does 3CMB Do

As a corporate compliance and controls monitoring function, 3CMB provides comprehensive risk-based monitoring of compliance with core policy, central directives, orders, and regulations. Compliance activity results are reported back to ministries and central agencies to promote prudent financial management and support our stakeholders achieve better program outcomes.

Why Our Work is Important

The compliance and monitoring function is a crucial component of the Province's financial management framework. It is a mechanism to identify and manage financial risks to support stakeholders achieve their objectives. 3CMB does this by:

- monitoring and reporting on compliance of government transactions
- recommending improvements to government policy, practices, training, and systems
- identifying risks and supporting stakeholders to strengthen their financial management practices
- providing custom transaction monitoring and reporting to mitigate unique or emerging risks
- reducing the cost of internal controls by implementing a risk-based monitoring approach

Who is this Report For

This report is intended for stakeholders with financial management monitoring, oversight, or governance roles and responsibilities. It demonstrates the Province's commitment to evaluate and report on financial management as a requirement under the *Financial Administration Act*. It also establishes benchmarking and promotes broader engagement of governance processes while supporting government's accountability and the public trust.

Summary of Compliance and Monitoring Activities

The Corporate Compliance Branch (3CMB) provides continuous monitoring of government's financial transactions to identify indicators of financial risk and compliance with policy. This report summarises 3CMB activities and outcomes for fiscal year 2023.

Key Summary

- Mitigated systematic fraud risks of one-time benefit and recovery programs
- Vast majority of government's transactions are low risk and well administered
- Procurement documentation and compliance continues to be a challenging area
- Event driven reporting administration indicates accuracy remained consistent
- Increased scope of 3CMB coverage and risk indicators
- Fraud risk assessments completed by all ministries

Mass Payment Monitoring

3CMB monitors government's one-time benefit and recovery programs for systemic fraud schemes or unexpected payment patterns acting as the last line of defence to mitigate risks.

Inherent program risks have been mitigated by ministries and OCG and no fraud schemes or abnormal payment patterns have been identified. All analytic results and outcomes are understood and explainable.

Compliance and Monitoring Activities

Monitoring and risk-based reviews of government's payments have returned to pre-pandemic volumes.

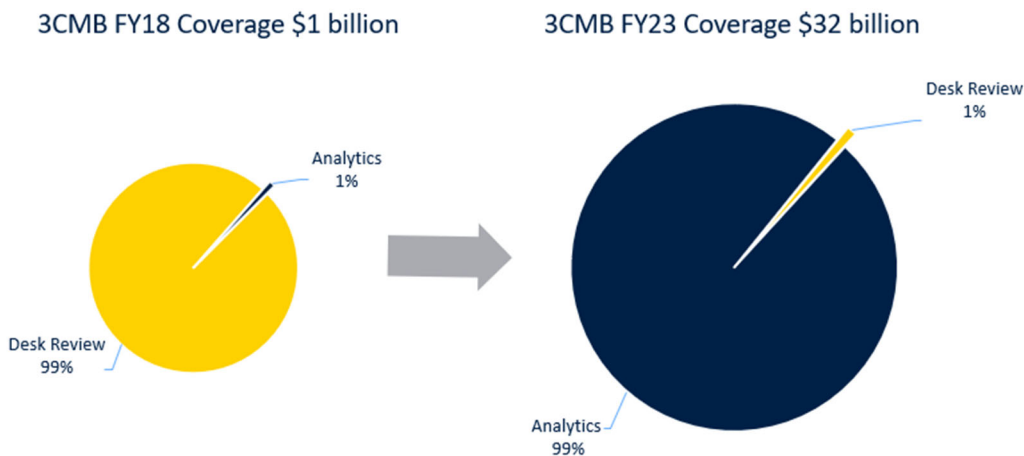
Over 99 percent of low-risk payment streams 3CMB monitored during the year were within expectations and did not raise any risks. Most of government's payments fall within this category and during the year 3CMB monitored \$32 billion of payments. These payments are typically to government's Crown organisations and agencies or long-term service providers of government.

Data analytics is also used to identify indicators of fraud or error, and control weaknesses. All payments are subject to these tests and during the year 1,014 payments were flagged for 3CMB review and approximately 483 payments were assessed as elevated risk and alerted to ministries for immediate action.

Most of the findings from 3CMB reviews relate to weaknesses in procurement documentation or approaches. This is not a new or emerging risk and is an inherently challenging area to improve upon and resolve. 3CMB works with ministries to address or mitigate many of these findings and risks.

Continuing from last fiscal, 3CMB analyzed and tested pandemic and the 2021 extreme weather event payments for compliance and reporting risk. In fiscal 2023, event driven testing expanded to cover the payments in support of displaced Ukrainian refugees. Sixty-three percent of the payments reviewed were correctly recorded and financial policy compliance was higher for these payments than routine government expense payments.

3CMB continues to build our compliance coverage across government. This year 3CMB expanded to include the revenue and receivable transactions. Data analytics monitoring continues to be the preferred approach due to its effectiveness and efficiency. Document reviews are time consuming for 3CMB and stakeholders and are only used when there are no alternatives. The graphic below illustrates these changes.



3CMB continues to invest in data analysis tools and resources as this approach as it's the most efficient and effective way to identify and respond to financial risks.

Forensic Accounting Services

During the year, 8 concerns about government’s financial administration were reported by individuals or BC Public Service employees. Each of these reports are reviewed, assessed, and appropriately actioned. The majority of these incidents have been closed and do not require a forensic accounting engagement to resolve.

Several fraud risk management tools have been provided to BC Public Service employees. These tools support employees in identifying and reporting fraud. 3CMB continues to work with ministries to develop and refine fraud risk assessment and mitigation strategies and tools.

Mass Payment Monitoring

In response to the unique risks inherent to governments pandemic response benefit and recovery payment programs, 3CMB implemented analytics monitoring and reporting to support the programs' existing financial controls and further mitigate financial risks.

Post-pandemic, we continue to use this monitoring capacity to support ministry programs with inherent risk of fraud or error.

Key Summary

- Inherent program risks have been mitigated
- No fraud schemes or abnormal payment patterns have been identified
- 3CMB analytics approach and tests are operating as planned and are effective
- Analytic results and outcomes are understood and explainable

Scope and Approach

During the year 3CMB worked with ministries to monitor payments for the following programs:

- EMCR Emergency Support Services Evacuee e-Transfer

3CMB also continued to monitor payments for the following previously established programs:

- BC Recovery Benefit
- COVID-19 Closure Relief Grant
- BC PST Rebate on Select Machinery and Equipment
- BC Increased Employment Incentive

These programs have inherent financial risk due to their large scope, multifaceted eligibility criteria and the Province's limited pre-existing relationship with the intended recipients. These factors and self-application design of such programs makes them an attractive target for fraudsters.

In response to these risks, 3CMB implemented daily analytic tests and reporting to support the programs' existing financial controls and further mitigate financial risks. The analytic tests assess payments for three risk categories that are described below.

Program Design and Business Rule Risks	<ul style="list-style-type: none"> • Failures can lead to large volumes of incorrect payments going undetected • Recovery of overpayments can be challenging
Multiple Payments Risks	<ul style="list-style-type: none"> • Fraud risk and further analysis is necessary to understand the results • Individual payments may be held pending resolution • Informs future actions such as audits or program design
Higher Risk Characteristics	<ul style="list-style-type: none"> • Patterns and trends identified based on program experience • Individual payments may be held pending resolution • Informs future actions

Monitoring Outcomes

Monitoring and reporting results shows that the government continues mitigate systemic and significant financial risks and still achieve program delivery objectives.

While 3CMB results indicate an overall low level of financial risk, it is reasonable to expect a small volume of ineligible payments did occur. 3CMB works with ministries to understand results in-depth and to mitigate risks. Ministries are planning and conducting audits to further confirm eligibility and recover any ineligible payments.

Compliance and Monitoring Activities

Key Summary

- Vast majority of government’s transactions are low-risk and well administered
- Procurement documentation and compliance continues to be a challenging area
- Administration of event driven expenses is working
- Increased scope of 3CMB coverage and risk indicators

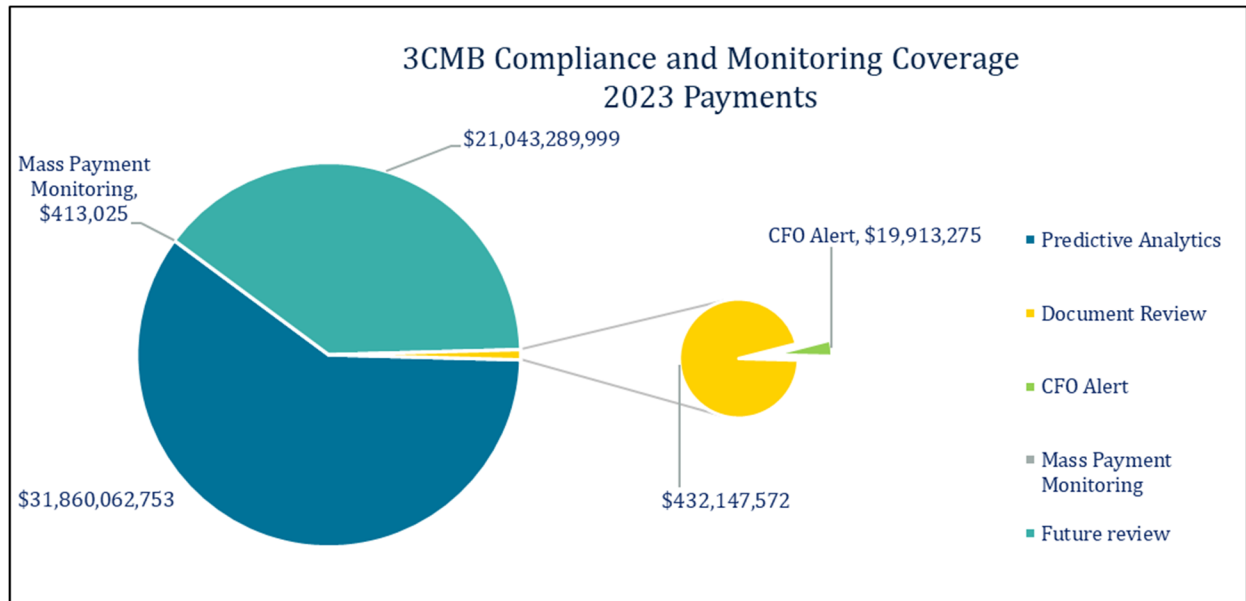
Scope and Approach

3CMB monitors payments out of the Corporate Financial System. These can be payments to government’s service providers, Crown corporations and agencies, and employees.

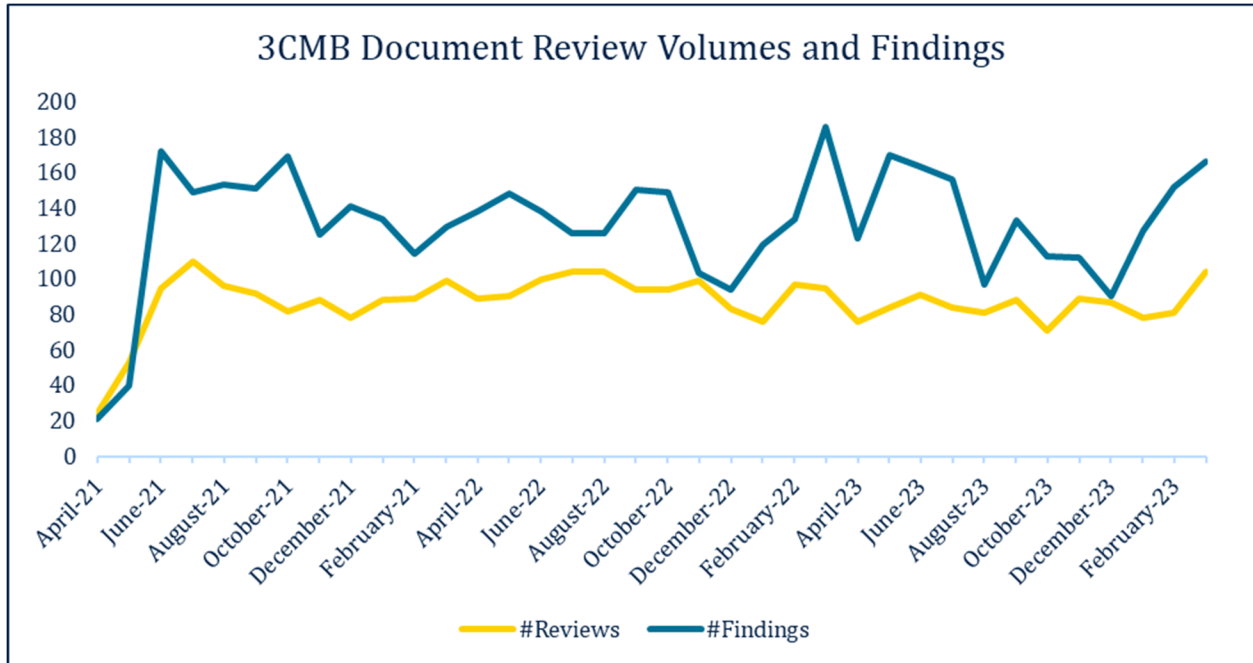
Each payment is monitored using risk-based criteria and pattern analysis. 3CMB uses the results to inform actions such as 3CMB document reviews, notification to the ministry CFO, or further research and assessment.

A monthly report on 3CMB activities and outcomes is provided to each ministry CFO. 3CMB works with ministries to resolve findings or mitigate risks.

The below graphic illustrates 3CMB’s compliance coverage for the fiscal year 2023.



Document reviews are time-consuming for 3CMB and stakeholders and are only used when there are no alternatives. Over the years 3CMB has reduced document reviews as analytic monitoring is built out and risks are better understood. Analytic coverage has significantly increased as 3CMB worked with ministries to identify suitable payment streams for inclusion.



At the onset of the COVID-19 pandemic 3CMB temporarily reduced document reviews and relied on increased analytic coverage. Information on 3CMB findings is discussed on the next page.

Predictive Analytics Results

3CMB uses predictive analytics to monitor 95 lower-risk ministry payment streams. These payments are typically to Crown corporations and agencies or long-term service providers of government.

Over 99 percent of low risk payment streams 3CMB monitored during the year were within expectations and did not raise any risks.

Predictive analytic is the most efficient and effective way to monitor payments and 3CMB continues to look for opportunities to expand it.

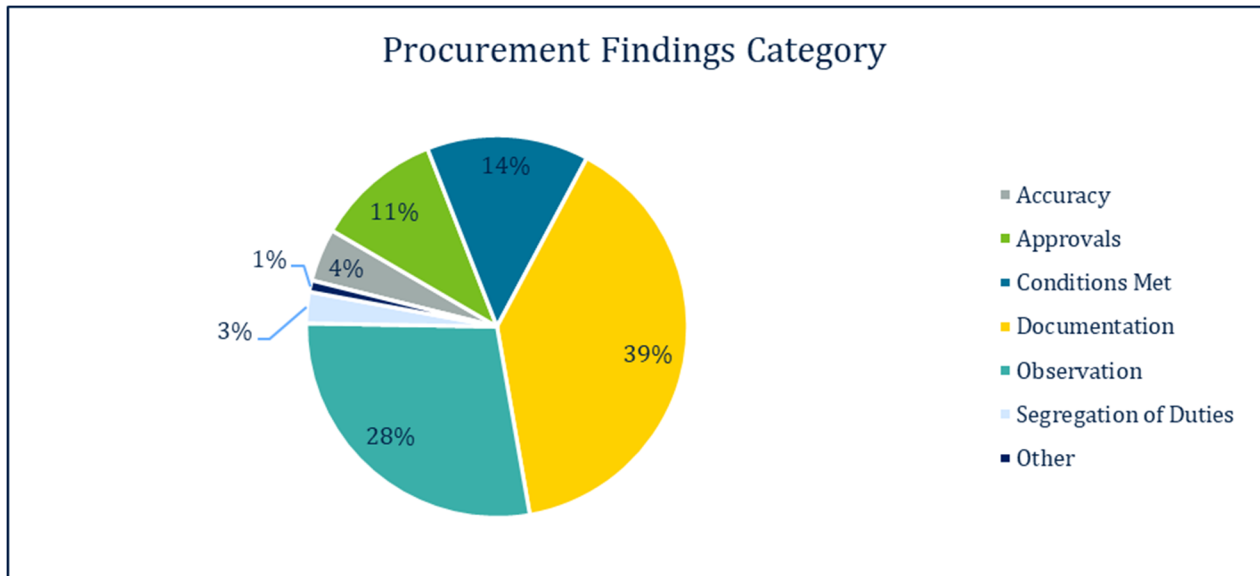
Document Review Results

Each month 3CMB uses analytics to select ministry payments for review. Ministries provide 3CMB with documents to support payments and 3CMB reviews them for compliance with government’s financial administration policies and indicators of risk.

In fiscal 2023 about 1,014 payments from all ministries were selected for a 3CMB document review.

Most of the findings from 3CMB reviews relate to weaknesses in procurement documentation or approaches. Specifically, weaknesses in procurement planning and management of contracts remains a persistent risk. This is not a new or emerging risk and is an inherently challenging area to improve upon and resolve. 3CMB works with ministries to address or mitigate many of these findings or risks.

See the figure below for procurement findings distribution by category for fiscal year 2023.



The findings distribution is broadly consistent across ministries and more closely related to the nature of the procurement than the ministries own processes or procedures. 3CMB continues to work with ministries and other central agencies to address these risks.

Event Driven Reporting

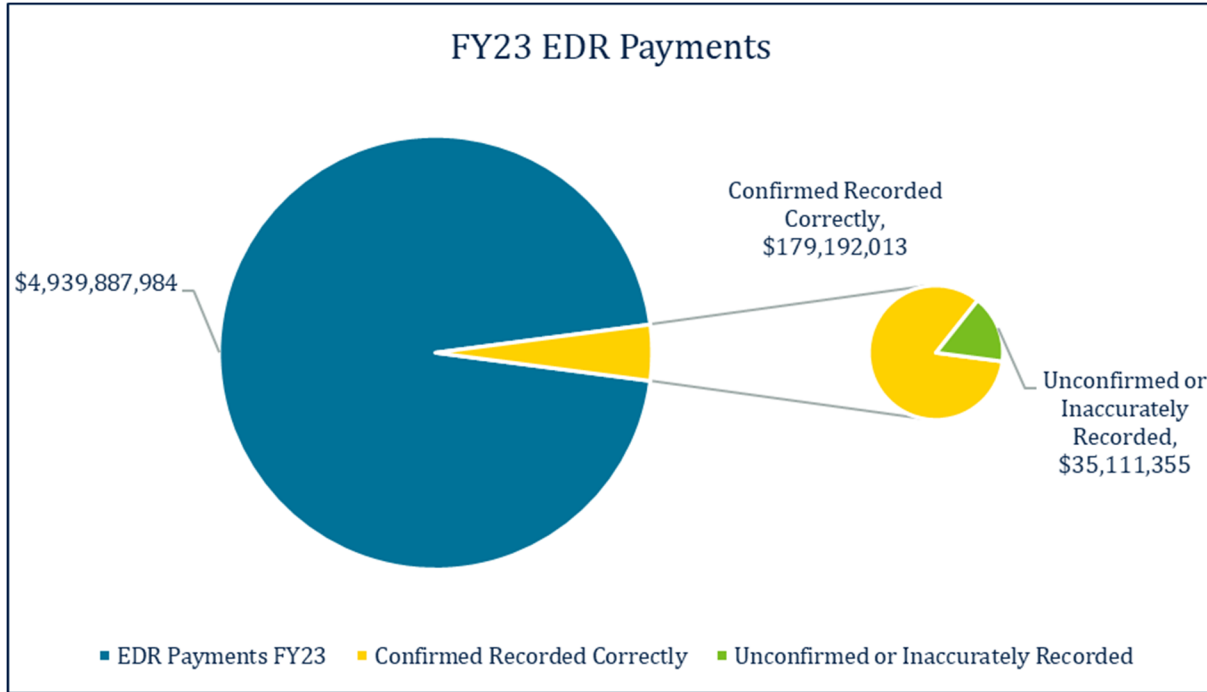
The Event Driven Financial Reporting (EDR) process identifies government’s direct expenditures associated with the COVID-19 pandemic, the 2021 atmospheric river weather event, and the displaced Ukrainian refugees. These expenditures are incremental to the regular business of government. EDR provides timely, deep, and reliable financial information to government decision-makers.

Summary EDR Payment Testing:

- Administration of EDR expenses accuracy remains consistent with the prior fiscal year
- Compliance with financial policies was higher for these payments than regular government expense payments, and higher than the previous fiscal year
- Monitoring and testing did not identify any systemic frauds schemes or internal control weaknesses

**FY23 Compliance and Monitoring
Annual Progress Report**

Starting in May 2020, 3CMB began to test COVID-19 payments for compliance and reporting risks. In March and May 2022, 3CMB also initiated testing on extreme weather payments and payments in support of displaced Ukrainian refugees. This testing continued through fiscal year 2023, and in collaboration with ministries, 3CMB was able to complete all 390 reviews as planned.



3CMB concluded that 10% or \$35 million of the EDR payments tested were either recorded inaccurately or could not be conclusively determined to be related to the event driven reporting used. When comparing review results to fiscal year 2022 at 11%, it indicates that the focus on processes and procedures for administration of these incremental costs has remained consistent.

Comparing the average finding per review, EDR reviews resulted in 172% less compliance findings than routine risk-based reviews, significantly improved from the previous fiscal year where 3% less compliance findings were noted. 3CMB attributes this outcome to efforts made in communicating to ministries the need to refocus on these programs after a decline last fiscal.

CFO Alerts

CFO Alerts are sent to ministry CFOs to notify them of potential higher risks that may need to be actioned to prevent loss or mitigate risks. Ministry CFOs are asked to make enquiries, act as needed, and advise 3CMB of the outcome. There were 483 transactions in fiscal 2023 that resulted in 169 CFO Alerts to 20 ministries. Of the 483 transactions escalated, 328 were confirmed as risks.

Summary of Confirmed FY23 CFO Alert Risks:

- \$16.5 million was alerted from CFS payment monitoring
 - \$11 million was alerted due to expense authority segregation of duties or inaccurate authority for approved payments
 - Nearly \$2.8 million related to multiple CFS payments with similar details that went to the same payee
 - \$2.6 million was alerted on compliance findings of procurement and contract management concerns
- \$58,000 was alerted from corporate card transaction monitoring
 - Majority of travel card alerts stemmed from overdue balances
 - Purchase card alerts related to possible personal purchases or inactive cardholder transactions

Expanding Compliance Coverage

During the year 3CMB expand the scope of compliance activities to include analysis and testing of revenue and receivables transactions with the purpose of assessing policy compliance and identifying any financial management risks that may exist.

The initial pilot review phase focused on the practices around revenue and receivables for the Employer Health Tax, Property Transfer Tax, and Carbon Tax programs in the Ministry of Finance.

3CMB reviewed 24 revenue and receivables transactions. The majority of reviews were compliant with policy. However, 3CMB did identify weaknesses around maintaining sufficient documentation to support appropriate segregation of duties and understanding of roles and responsibilities for reconciling CFS balances to revenue bank accounts. 3CMB is supporting the ministry in addressing these risks.

Looking ahead, 3CMB will continue to increase focus on areas that have consequential risk for government. In the coming months 3CMB plans to initiate analysis and reviews for government programs that have significant reliance on qualified receiver due diligence. Appendix A provides more information on 3CMB initiatives.

Internal Control Framework

During the year, OCG undertook a comprehensive review of the Province's internal controls with the intent of defining a cross-government internal control framework. OCG will use the framework to support the ongoing design and monitoring of internal controls and provide practical guidance for central agencies and ministries to design, implement, operate, and maintain internal controls in consistent and structured manner.

The framework will be implemented across ministries in fiscal 2024 and will be incorporated into the supporting basis behind managements representations for the Public Accounts.

Supporting and monitoring this implementation will be the basis for 3CMBs compliance approach going forward for several years.

Forensic Accounting Services

Key Summary

- Most concerns reported do not establish a financial loss or control weakness
- OCG has established an effective fraud risk management framework
- Fraud risk assessments completed by all ministries
- Fraud Awareness and Prevention eLearning taken by more than 85% of ministry staff
- Fraud Risk Management resources support ministries and crown corporations

Background and Objectives

The Comptroller General is responsible for the overall quality and integrity of government’s financial management and control systems. This includes responding to financial risks identified and reported across government and leading fraud prevention and detection initiatives. This report provides a status update on open financial risks reported to OCG as well as current fraud awareness initiatives.

Financial Risks Reported

During the year, 8 concerns about government’s financial administration were reported by citizens or BC Public Service employees. Each of these reports are reviewed and assessed and appropriately actioned.



One financial concern reported resulted in a forensic engagement to assess the potential risk exposure to government where oversight of front-line staff was not sufficient.

It was determined for all closed incidents that there did not appear to be a direct financial loss identified or systemic internal control weaknesses.

In some instances, Forensic Accounting Services (FAS) refers the concern to another agency within government or to another branch of OCG such as internal audit, compliance, policy, or accounting.

Fraud Awareness Initiatives

An effective fraud risk management program enables the government to have controls that first prevent fraud from occurring, detect as soon as a fraud happens, and respond effectively to fraud incidents when they occur.

Summary of Fraud Awareness Initiatives

- Fraud Risk Management Toolkit
 - Guide to help ministry and crown agency decision-makers respond to fraud risks
- Fraud Awareness and Prevention eLearning
 - Walks learners through what fraud is, how to prevent and detect fraud, and how to report fraud
- Fraud Risk Assessments
 - Identify an organization's vulnerabilities to internal and external fraud

Preventative controls are important because they are designed to reduce the risk of fraud and misconduct from occurring in the first place. While government has sound legislation and policies in place for addressing fraud incidents, there is opportunity in taking a preventative approach; and along the way support more consistent and appropriate outcomes when incidents do occur.

A preventative focus up front results in less time and effort spent on the back-end response side. To that end our belief is that education is a foundational building block to enhance our preventative measures.

FAS has implemented the following initiatives to advance preventative controls across government.

1. Fraud Risk Management Toolkit

The Fraud Risk Management toolkit is an internal guide to help ministry decision-makers respond to fraud risks.

The toolkit is broken down into four phases and provides start to finish direction on how to respond to fraud risks. This document helps to ensure that a consistent approach is used across government when responding to fraud risks.

The toolkit was provided to all employees and is accessible on the OCG intranet.

2. Fraud Awareness and Prevention eLearning

FAS worked with the PSA to develop the Fraud Awareness and Prevention eLearning which launched in June 2021.

The course walks learners through what fraud is, how to prevent and detect fraud, and how to report fraud. It provides learners with scenarios to put the learning in context.

FAS is asking all employees to take this course at least once every 3 years. To date, more than 85% of core government employees have completed the course.

3. Fraud Risk Assessments

Fraud risk assessments proactively identify an organization's vulnerabilities to internal and external fraud. Based on the results, mitigation strategies can be developed to reduce the risk to an acceptable level.

FAS consulted with ministry CFOs on the design and rollout across ministries.

Ministries completed their fraud risk assessment in Feb 2023. These initial results were compiled showing no new or unknown risks.

The completion of a cross-government fraud risk assessment is an important milestone creating a baseline to build on and refine through further iterative fraud risk assessment activities.

4. Fraud Risk Management Resources Site

OCG has made the fraud risk management resources we developed available to help inform and support organizations outside of core government. The resources have been customized to be relevant to any size organization and any degree of sophistication on fraud risk management.

Fraud Risk Management Framework

During the year, OCG assessed the state of governments Fraud Risk Management Framework considering activities and processes around fraud prevention and detection (Appendix B).

The result of the assessment showed OCG has established an effective fraud risk management framework that is designed to be comprehensive in addressing both preventative and detective aspects of fraud risk management.

The Office of the Auditor General also reviewed government's fraud risk management approach. Their report was released in March 2022 demonstrating significant improvements to all aspects of government's Fraud Risk Management Framework.

Appendix A: Compliance and Monitoring Initiatives Update

Compliance and monitoring activities are evolving to address emerging risks and take advantage of new capacity and technology. The following initiatives are in process by 3CMB.

Activity	Date Range	Project Phase	Status
Event Driven Reporting Monitoring	May 2020 – Ongoing	Operational	✓
Monthly selection of payments and journal vouchers coded to Event Driven Reporting project codes to confirm classification and compliance with policy.			
BC Recovery Benefit	Dec 2020 – Jun 2023	Operational	✓
Mass payment monitoring for logic, error and fraud risks.			
BC PST Rebate on Select Machinery and Equipment	Apr 2020 – Jun 2023	Operational	✓
Mass payment monitoring for logic, error and fraud risks.			
BC Increased Employment Incentive	Apr 2020 – Jun 2023	Operational	✓
Mass payment monitoring for logic, error and fraud risks.			
Manual Journal Entry Monitoring	Oct 2020 – Ongoing	Operational	✓
Monthly selection of General Ledger transactions to review supporting documentation and confirm compliance with policy.			
Capital Asset Monitoring	Dec 2020 – Ongoing	Operational	✓
Data based analysis and testing of capital asset transactions to support a targeted review.			
EMCR Targeted Review	May 2021 – Ongoing	Operational	✓
Data analysis and testing to assess EMCR's current financial control and policy compliance status.			
Fuel Card Targeted Review	Jun 2021 – Ongoing	Operational	✓
Data based analysis of government fuel card usage to identify and mitigate policy and fraud risks.			
Supplier Banking Changes Targeted Review	Jun 2021 – Ongoing	Operational	✓

**FY23 Compliance and Monitoring
Annual Progress Report**

Activity	Date Range	Project Phase	Status
Data based analysis of changes to supplier banking details to identify and mitigate policy and fraud risks.			
Revenue Monitoring	Dec 2022 – Ongoing	Operational	✓
Data based analysis of revenue transactions to support launching a targeted review. Research and implementation phase.			
EMCR Emergency Support Services e-Transfer Monitoring	Aug 2022 – Ongoing	Operational	✓
Mass payment monitoring for logic, error and fraud risks.			
Qualified Receiver Targeted Review	Feb 2023 – May 2023	Planning	✓
Data based analysis of higher risk QR reliance to identify and mitigate policy and fraud risks.			



On track



Delayed/potential delay



Risks/roadblocks identified

Appendix B: Fraud Risk Management Framework Assessment

Fraud Risk Management Framework Assessment

March 3, 2023

Prepared for: Comptroller General



Ministry of
Finance

Table of Contents

Purpose 3

Background 3

Fraud Risk Management Framework Assessment 3

Assessment Results 4

Appendix A: Fraud Prevention Scorecard..... 5

Appendix B: Fraud Detection Scorecard 10

Appendix C: COSO Fraud Risk Management Principles and Alignment to OCG and Cross-Government Activities 14

Fraud Risk Management Framework Assessment

Purpose

To assess the effectiveness of the Office of the Comptroller General's (OCG) fraud risk management framework.

Background

A proactive approach to managing fraud risk is one of the best steps an organization can take to mitigate exposure. Although it is not economically feasible to eliminate all fraud risk, proactive and constructive steps can be taken. The combination of effective fraud risk governance, a thorough fraud risk assessment, and strong fraud prevention and detection measures, along with coordinated and timely investigations and corrective actions, can significantly mitigate fraud risks.

OCG's approach to establishing a fraud risk management framework began by first clarifying roles and responsibilities for fraud prevention and detection in cross-government functions responsible for governance over government's financial management framework. As these cross-government functions built further capacity over fraud risk management, a fraud awareness campaign was launched to inform government decision makers and employees of their roles and responsibilities in managing fraud risk and reporting incidents of actual or suspected fraud.

OCG has also developed and distributed several tools that government organizations use to inform themselves on fraud risks and how to prevent and respond to them. These tools also facilitate the completion and amalgamation of a cross-government fraud risk assessment overseen by OCG to inform purposeful, coordinated, and efficient corporate action in response to fraud risks.

These actions are supported by a reporting process within OCG to facilitate management of the fraud risk management framework in conjunction with reporting to the Deputy Ministers Audit Committee.

Fraud Risk Management Framework Assessment

OCG conducted its assessment based on a guide available from the Office of the Auditor General of Canada. The assessment considers organizational activities and processes around fraud prevention (Appendix A) and fraud detection (Appendix B) and provides a comprehensive overview.

The assessment was completed by OCG's Corporate Compliance and Controls Monitoring branch and put through an internal quality assurance review.

Assessment Results

OCG has established an effective fraud risk management framework that is designed to be comprehensive in addressing both preventative and detective aspects of fraud risk management. The completion of a cross-government fraud risk assessment is an important milestone in this process and is a starting baseline to build on and refine through further iterative fraud risk assessment activities.



Prepared by: Xing Zheng, Assurance Manager

March 3, 2023



Reviewed by: Charles Mutanda, Executive Director

March 3, 2023



QA Reviewer: Alex Kortum, Executive Director

March 23, 2023



Approved by: Carl Fischer, Comptroller General

March 24, 2023

Fraud Risk Management Framework Assessment

Appendix A: Fraud Prevention Scorecard

This scorecard is used to assess OCG's fraud risk management framework and is completed as part of an iterative fraud risk assessment to assess government's fraud prevention system. Each area, factor, or consideration is scored to determine if further action is required in maintaining or improving fraud prevention activities.



Red: indicating that the area, factor, or consideration needs substantial strengthening and improvement to bring fraud risk down to an acceptable level.








Yellow: indicating that the area, factor, or consideration needs some strengthening and improvement to bring fraud risk down to an acceptable level.






Green: indicating that the area, factor, or consideration is strong and fraud risk has been reduced (at least) to a minimally acceptable level.

No.	Fraud prevention area, factor, or consideration	Score	Notes	Action item	Ref (App C)
P1	Our organizational culture—tone from the top—is as strong as it can possibly be and establishes a zero-tolerance environment with respect to fraud.		<ul style="list-style-type: none"> - Financial Administration Act - CPPM 20.4 Fraud Risk Management Policy - Communications from Comptroller General (CG) - eLearning/fraud awareness tools 	None at this time	1A, 1B, 1C, 1D, 1E, 1F, 3B, 3F, 3G, 3N, 3O, 5D
P2	Our organization's top management consistently displays the appropriate attitude regarding fraud prevention and encourages free and open communication regarding ethical behaviour.		<ul style="list-style-type: none"> - Financial Administration Act - CPPM 20.4 Fraud Risk Management Policy - Communications from OCG - eLearning/fraud awareness tools 	None at this time	1A, 1B, 1C, 1D, 1E, 1F, 3B, 3F, 3G, 3N, 3O, 5D
P3	Our code of conduct has specific provisions that address and prohibit inappropriate relationships whereby members of our Executive Committee or members of management could use their position for personal gain or other inappropriate purposes.		BC Public Service employees are required under the Public Service Oath Regulations and Standards of Conduct to avoid conflicts of interest. They have an obligation to proactively disclose information to their manager (or ethics advisor) regarding real, perceived, or potential conflict of interest so that any such conflict may be assessed and appropriately addressed.	None at this time	1B, 1C, 1D, 1E
P4	We have done a rigorous fraud risk assessment using the COSO Enterprise Risk Management Integrated Framework and have taken specific actions to strengthen our prevention mechanisms as necessary.		<ul style="list-style-type: none"> - Fraud Risk Assessment Toolkits prepared by ministries - Results compiled annually and validated as part of an iterative process 	1. Continue with iterative fraud risk assessment activities	3C, 3D, 3E






Fraud Risk Management Framework Assessment

No.	Fraud prevention area, factor, or consideration	Score	Notes	Action item	Ref (App C)
P5	We have addressed the strengths and weaknesses of our internal control environment adequately and have taken specific steps to strengthen the internal control structure to help prevent the occurrences of fraud.		<ul style="list-style-type: none"> - Fraud Risk Management Program - 3CMB compliance monitoring (CFO/CG Reporting, CFO alerts, etc.) - 3CMB compliance monitoring incorporating risk-based approach and leveraging near-time/date centric risk detection - 3CMB COVID-19 support and economic recovery mass payments monitoring - IAAS financial risk and control reviews - IAAS audit plan and reports - FRAS CFO letters of representation - FRAS JV review - Fraud awareness campaign - formal communication regarding fraud prevention, responsibilities, and announcement of tools launched 	None at this time	3A, 3C, 3D, 3E, 3G, 3H, 3I, 3J, 3K, 3L, 3M, 3O
P6	We have assessed the alignment of authorities and responsibilities at all levels of organizational management and are not aware of any misalignments that might represent vulnerabilities to fraud.		<ul style="list-style-type: none"> - CPPM 20.4 Fraud Risk Management Policy - Financial Administration Act - Fraud Risk Management Toolkit - FAS operating procedures – Dec 15, 2020 - Joint Investigation Protocol - Monthly reporting to CG/DMAC 	None at this time	1A, 3C, 4C, 4D, 4E
P7	Our Audit Committee has taken a very proactive posture with respect to fraud prevention.		OCG reports to a DMAC, which provides oversight of the internal audit function and financial management framework for the benefit of government and Treasury Board. DMAC approved and supports OCG's fraud risk management plan	None at this time	3A, 5D
P8	Our Audit Committee is composed only of independent members and includes persons with financial accounting and reporting expertise.		DMAC is comprised of senior staff for across ministries with financial accounting and reporting expertise and responsibilities	None at this time	
P9	Our Audit Committee meets at least quarterly and devotes substantial time to assessing fraud risk and proactively implementing fraud prevention mechanisms.		DMAC meets monthly and receives reporting from the Comptroller General on financial management initiatives including the status and direction of OCG's fraud risk management plan	None at this time	3A, 5A, 5D




Fraud Risk Management Framework Assessment

No.	Fraud prevention area, factor, or consideration	Score	Notes	Action item	Ref (App C)
P10	We have a strong internal audit function that operates independently of management. The charter of our internal audit function expressly states that the internal audit team will help prevent and detect fraud and misconduct.		IAAS provides a wide range of internal audit and consulting services to ministries and the broader public sector. IAAS provides independent and objective assurance and advice to support effective financial management, governance, accountability, and performance management practices in government. IAAS reports to a DMAC, which provides oversight of the internal audit function for the benefit of government and Treasury Board. Some ministries have their own internal audit departments. These departments focus on compliance with specific legislation and Ministry policies and procedures.	None at this time	3K, 5A, 5D
P11	We have designated an individual with the authority and responsibility for overseeing and maintaining our fraud prevention programs and have given this individual the resources needed to manage our fraud prevention programs effectively. This individual has direct access to the Audit Committee.		Comptroller General supported by OCG Executive and ministry CFOs	None at this time	3A, 3B, 5A, 5D
P12	Our Human Resources function conducts background investigations with the specific objective of assuring that persons with inappropriate records or characters inconsistent with our corporate culture and ethics are identified and eliminated from the hiring process.		<p>Security screening checks the history and background of successful applicants and current employees.</p> <p>Three levels of security screening exist:</p> <ul style="list-style-type: none"> - BC Public Service Criminal Record Check is required for all designated positions. - Criminal Records Review Act Check is required for applicants or current employees working with vulnerable citizens. - Enhanced Security Screening includes a higher level of criminal record check plus additional checks that may be required for the position. <p>Screening is mandatory for all designated positions in the BC Public Service. Hiring managers are responsible for confirming if and when screening is required. If an applicant or employee doesn't consent to screening, they can't be offered the position.</p>	None at this time	1B, 1C, 1D, 1E, 1F

Fraud Risk Management Framework Assessment

No.	Fraud prevention area, factor, or consideration	Score	Notes	Action item	Ref (App C)
P13	Personnel involved in the financial reporting process have been assessed with regard to their competencies and integrity and have been found to be of the highest calibre.		<p>The BC Public Service hiring process is driven by competency assessment and requires the best qualified individual be hired for positions. Job requirements are strictly controlled, and the hiring process is supported by segregated recruitment staff at the PSA. Positions with financial management and reporting responsibilities are assessed for the requirement to hold a professional accounting designation in good standing.</p> <p>This process is further supported by annual declarations and standards of conduct reviews and the conduct and professional development requirements by the professional accounting bodies.</p>	None at this time	1B, 1C, 1D, 1E
P14	All our employees, vendors, and contractors have been made aware of our zero-tolerance policies related to fraud and are aware of the appropriate steps to take in the event that any evidence of possible fraud comes to their attention.		<p>Communicated by:</p> <ul style="list-style-type: none"> - Fraud awareness campaign - Fraud awareness eLearning (mandatory course 80%+ coverage) 	<ol style="list-style-type: none"> 1. Consider communication strategy for vendors 2. Consider refresh cycle of fraud awareness campaign 	1B, 1C, 1D, 1E, 3D, 3O
P15	We have a rigorous program for communicating our fraud prevention policies and procedures to all employees, vendors, contractors, and business partners.		<p>Communicated by:</p> <ul style="list-style-type: none"> - Fraud awareness campaign - Fraud awareness eLearning (mandatory course 80%+ coverage) 	<ol style="list-style-type: none"> 1. Consider communication strategy for vendors 2. Consider refresh cycle of fraud awareness campaign 	1B, 1C, 1D, 1E, 3D, 3O
P16	We have policies and procedures in place for authorization and approval of certain types of transactions and for certain values of transactions to help prevent and detect the occurrences of fraud.		<p>Outlined in the Core Policy and Procedure Manual and supported by access and application controls and monitoring of the financial management framework by OCG and ministry CFOs.</p>	None at this time	
P17	Our performance measurement and evaluation process include elements specifically addressing ethics and integrity as well as adherence to the Values and Ethics Code for the Public Sector and the OAG's Code of Values, Ethics and Professional Conduct.		<p>Mandatory annual review of the Standards of Conduct and Oath of Employment for all BC Public Service employees. The latest stats provided by PSA showed a completion rate of 90.7%</p>	None at this time	1B, 1C

Fraud Risk Management Framework Assessment

No.	Fraud prevention area, factor, or consideration	Score	Notes	Action item	Ref (App C)
P18	We have an effective whistleblower protection program in place, and its existence and procedures are known to all employees, vendors, contractors, and partners.		BC's Public Interest Disclosure Act (PIDA) provides a safe, legally protected way for current and former BC public sector employees to report serious or systemic issues of wrongdoing to their supervisor, a designated officer or to the Ombudsperson. PIDA prohibits retaliation against employees who speak up about potential wrongdoing in the public sector.	1. Consider procedures for vendors	1F
P19	We review the above fraud preventive mechanisms on an ongoing basis and document these reviews as well as the communication with the Audit Committee regarding areas that need improvement.		<ul style="list-style-type: none"> - Monthly and annual progress reports to CG and feedback - Fraud Awareness and Prevention eLearning preparation and feedback cycle and stats monitoring - FAS projects and assessment results, debrief, and lessons learned - Monthly and annual reporting to DMAC and feedback received 	None at this time	5A, 5B, 5C, 5D
P20	We have a fraud response plan in place and know how to respond if a fraud allegation is made. The fraud response plan considers <ul style="list-style-type: none"> - who should perform the investigation - how the investigation should be performed - when a voluntary disclosure to the government should be made - how to determine the remedial action - how to remedy control deficiencies identified - how to administer disciplinary action 		Detailed instructions are documented in the FAS Operating Procedures	None at this time	4C

Fraud Risk Management Framework Assessment

Appendix B: Fraud Detection Scorecard

This scorecard is used to assess OCG's fraud risk management framework and is completed as part of an iterative fraud risk assessment to assess government's fraud detection system. Each area, factor, or consideration is scored to determine if further action is required in maintaining or improving fraud detection activities.



Red: indicating that the area, factor, or consideration needs substantial strengthening and improvement to bring fraud risk down to an acceptable level.








Yellow: indicating that the area, factor, or consideration needs some strengthening and improvement to bring fraud risk down to an acceptable level.








Green: indicating that the area, factor, or consideration is strong and fraud risk has been reduced (at least) to a minimally acceptable level.

No.	Fraud detection area, factor, or consideration	Score	Notes	Action item	Ref (App C)
D1	We have integrated our fraud detection system with our fraud prevention system in a cost-effective manner.		Financial risk reporting to OCG from various sources are assessed and mitigation actions are taken in response via monitoring and/or internal control enhancements by OCG or at ministries. This process informs OCG's risk-based approach to financial management.	None at this time	2A, 3B, 3C, 3D, 3E, 3F, 3G, 3K, 3O
D2	Our fraud detection processes and techniques pervade all levels of responsibility within our organization, from the Audit Committee, to managers at all levels, to employees in all areas of operations.		OCG fraud detection is developed and supported by: <ul style="list-style-type: none"> - Fraud awareness campaign - Fraud awareness eLearning (mandatory course 83% coverage) - Fraud risk management toolkit to CFOs - Fraud risk assessment - 3CMB risk-based analytics monitoring and compliance reviews - IAAS financial risk and controls reviews - IAAS audit plan and reports - FRAS JV review - Reporting to CG and DMAC 	1. Continue with iterative fraud risk assessment activities	2A, 3B, 3C, 3D, 3E, 3F, 3G, 3K, 3M, 3O
D3	Our fraud detection policies include communicating to employees, vendors, and stakeholders that a strong fraud detection system is in place, but certain critical aspects of these systems are not disclosed to maintain the effectiveness of hidden controls.		Communicated by: <ul style="list-style-type: none"> - Fraud awareness campaign - Fraud awareness eLearning (mandatory course 80%+ coverage) 	1. Consider communication strategy for vendors 2. Consider refresh cycle of fraud awareness campaign	3D, 3O
D4	We use mandatory vacation periods or job rotation assignments for employees in key finance and accounting control positions.		Mandatory annual vacation is a requirement under HR policy administered by the PSA	None at this time	



Fraud Risk Management Framework Assessment

No.	Fraud detection area, factor, or consideration	Score	Notes	Action item	Ref (App C)
D5	We periodically reassess our risk assessment criteria as our organization grows and changes to make sure we are aware of all possible types of fraud that may occur.		Financial risk reporting to OCG from various sources are assessed and mitigation actions are taken in response via monitoring and/or internal control enhancements by OCG or at ministries. This process informs OCG's risk-based approach to financial management.	None at this time	2A, 3B, 3C, 3D, 3E, 3F, 3G, 3K, 3O
D6	Our fraud detection mechanisms place increased focus on areas in which we have concluded that preventive controls are weak or are not cost-effective.		OCG conducts audits, compliance reviews, and data analytics monitoring driven by known and emerging risks identified as part of continuous improvement and efficient and effective use of resources. OCGs fraud risk assessment process is iterative and will be refined over time to identify emerging areas of weakness.	1. Continue with iterative fraud risk assessment activities	2A, 3G, 3H, 3J, 3K
D7	We focus our data analysis and continuous auditing efforts based on our assessment of the types of fraud schemes to which organizations like ours are susceptible.		OCG audits and compliance reviews and data analytics monitoring are driven by known and emerging risks identified as part of continuous improvement and efficient and effective use of resources. Risk identification comes from other branches of OCG, ministry CFOs, and FAS activities among others.	None at this time	2A, 3G, 3H, 3J, 3K
D8	We take steps to ensure that our detection processes, procedures, and techniques remain confidential so that ordinary employees—and potential fraud perpetrators—do not become aware of their existence.		OCG detection processes are maintained at the branch level and reporting out consists of observations around risk as opposed to detection techniques.	None at this time	
D9	We have comprehensive documentation of our fraud detection processes, procedures, and techniques so that we maintain our fraud detection vigilance over time and as our fraud detection team changes.		OCGs fraud risk management plan is documented and supported by branch level risk assessment processes that are also documented.	None at this time	3A, 3C, 3D, 3E, 3G, 3H, 3I, 3J, 3K, 3L, 3M, 4A, 4C, 4D

Fraud Risk Management Framework Assessment

No.	Fraud detection area, factor, or consideration	Score	Notes	Action item	Ref (App C)
D10	Our information systems/IT process controls include controls specifically designed to detect fraudulent activity, as well as errors, and include reconciliation, independent review, physical inspections/counts, analysis, audits, and investigations.		The corporate financial system incorporates effective access and application controls with audit trails. This is supported by change management controls with appropriate corporate oversight, segregated financial risk and controls reviews, segregated internal controls monitoring through exception reports and data analytics monitoring, and segregated corporate compliance reviews and audits.	None at this time	3G, 3H, 3J
D11	Our data analysis programs focus on journal entries and unusual transactions, and transactions occurring at the end of a period or those that were made in one period and reversed in the next.		OCG compliance review of manual journal entries are driven by data and informed by FRAS's risk assessment results on financial reporting	None at this time	3G
D12	Our data analysis programs identify journal entries posted to revenue or expense accounts that improve net income or otherwise serve to meet analysts' expectations or incentive compensation targets.		OCG compliance review of manual journal entries are driven by data and informed by FRAS's risk assessment results on financial reporting	1. Continue to enhance JV compliance reviews based on FRAS risk assessments	3G, 3M
D13	We have systems designed to monitor journal entries for evidence of possible management override efforts intended to misstate financial information.		- 3CMB compliance review of manual journal entries - FRAS review of adjusting journal entries	None at this time	3G, 3M
D14	We use data analysis, data mining, and digital analysis tools to (a) identify hidden relationships among people, organizations, and events; (b) identify suspicious transactions; (c) assess the effectiveness of internal controls; (d) monitor fraud threats and vulnerabilities; and (e) consider and analyze large volumes of transactions on a real-time basis.		OCG compliance monitoring uses a risk-based approach and leverages near time/data centric risk detection mechanisms to monitor and report on financial and policy compliance risks. This process is nimble and responsive to emerging risks (for example pandemic response mass payments) and project-based assessment of data, scenarios, etc. OCG uses data centric analysis to assess financial risks for further corporate action.	1. Continue to expand policy compliance and analytics scope coverage	3G, 3H, 3I

Fraud Risk Management Framework Assessment

No.	Fraud detection area, factor, or consideration	Score	Notes	Action item	Ref (App C)
D15	<p>Our fraud detection documentation identifies the individuals and services responsible for:</p> <ul style="list-style-type: none"> - designing and planning the overall fraud detection process - designing specific fraud detective controls - implementing specific fraud detective controls - monitoring specific fraud detective controls and the overall system of these controls for realization of the process objective - receiving and responding to complaints related to possible fraudulent activity - investigating reports of fraudulent activity - communicating information about suspected and confirmed fraud to appropriate parties - periodically assessing and updating the plan for changes in technology, processes, and organization 		<p>OCG's fraud risk management framework is supported by core policy that outline roles, responsibilities and avenues of reporting in response to actual or suspected fraud.</p> <p>Key support roles in the process have documented operating procedures on intake, assessment, action, and reporting of incidents.</p> <p>As part of this, OCG also takes mitigating action via monitoring and/or internal control enhancements by OCG or at ministries. This process informs OCG's risk-based approach to financial management.</p>	None at this time	1A, 3A, 3C, 3D, 3F, 3O, 4C, 4D, 5A, 5D
D16	<p>We periodically assess the effectiveness of our fraud detection processes, procedures, and techniques; document these assessments; and revise our processes, procedures, and techniques as appropriate.</p>		<ul style="list-style-type: none"> - Fraud prevention and detection scorecard - Monitoring completion statistics of mandatory Fraud awareness eLearning - Iterative fraud risk assessment activities - Ongoing enhancements to risk detection mechanisms within OCG branches in response to changing and emerging risks 	None at this time	3D, 3E, 3G, 3H, 3I, 3J, 3K, 3L, 3M

Appendix C: COSO Fraud Risk Management Principles and Alignment to OCG and Cross-Government Activities

Purpose: To map OCG Fraud Risk Management activities and other supporting cross-government functions as they apply to the COSO FRM guide principles.

[COSO-Fraud Risk Management Guide](#)

[Ethics & Standards of Conduct in the BC Public Service - Province of British Columbia](#)

Principle 1: Establish a fraud risk management policy as part of organizational governance

- 1A CPPM 20.4 Fraud Risk Management Policy
- 1B Oath of Employment
- 1C Standards of Conduct
- 1D Corporate values of the BC public service
- 1E Conflict of interest guidelines
- 1F Public Interest Disclosure Act

Principle 2: Perform a comprehensive fraud risk assessment

- 2A Fraud Risk Assessment Toolkits prepared by ministries
Results are compiled annually and validated as part of an iterative process. The compiled results inform where further fraud risk assessment activities may be required. This is supported by other OCG activities (listed under Principle 3. Below)

Principle 3: Select, develop, and deploy preventative and detective fraud control activities

- 3A BN to CG March 31, 2020 re: approval to initiate advancement of Fraud Risk Management Program (FRMP). Includes:
 - Details for FRMP plan
 - Roles and responsibilities (FAS, FMB, IAAS, PSA, Ministry CFOs)
 - Consideration of risks
- 3B Presentations (DMAC, FOAC, CFO Council, Comms Council, etc.)
- 3C Fraud Risk Management Toolkit
- 3D Fraud Awareness and Prevention eLearning
- 3E Fraud Risk Assessment
- 3F Policy Practice sent to all ministries (e.g. phishing schemes)
- 3G 3CMB compliance monitoring (CFO/CG reporting, CFO alerts, etc.)
- 3H 3CMB compliance monitoring incorporating risk-based approach and leveraging near time/data centric risk detection
- 3I 3CMB COVID-19 support and economic recovery mass payments monitoring
- 3J IAAS Financial Risk and Control Reviews
- 3K IAAS audit plan and reports
- 3L FRAS CFO letters of representation
- 3M FRAS JV review
- 3N OCG intranet
- 3O Fraud awareness campaign – A series of formal communications regarding fraud prevention, responsibilities, and announcement of tools launched (FRM toolkit, eLearning, website)

Fraud Risk Management Framework Assessment

Principle 4: Establish a fraud reporting process and coordinated approach to investigation and corrective action

- 4A CPPM 20.4 Fraud Risk Management Policy
- 4B Fraud Risk Management Toolkit
- 4C FAS operating procedures
- 4D Joint Investigation Protocol
- 4E Monthly reporting to CG/DMAC

Principle 5: Monitor the fraud risk management process, report results, and improve the process

- 5A Monthly and annual progress reports to CG and feedback
- 5B Fraud Awareness and Prevention eLearning preparation/feedback cycle and stats monitoring
- 5C FAS projects and assessment results, debrief, and lessons learned
- 5D Monthly and annual reporting to DMAC and feedback received
- 5E Fraud prevention and detection scorecard