



OFFICE OF THE COMMISSIONER OF POLICE

Report to those charged with governance on the 2023 financial audit

October 2024

*To help the public service
spend wisely*

TABLE OF CONTENTS

INTRODUCTION	4
AUDITORS RESPONSIBILITIES IN RELATION TO THE AUDIT.....	4
Auditor’s responsibility under International Standards on Auditing.....	4
Responsibilities of Management and Those Charged With Governance	5
Other information in documents containing audited financial statements:.....	5
CONDUCT, APPROACH AND OVERALL SCOPE OF THE AUDIT.....	5
AUDIT REPORT, ADJUSTMENTS AND MANAGEMENT REPRESENTATION	5
SIGNIFICANT FINDINGS FROM THE AUDIT	5
Significant accounting practices	5
Management’s judgments and accounting estimates.....	6
Going concern doubts.....	6
Significant and other deficiencies in internal control.....	6
Fraud or illegal acts.....	6
Significant difficulties encountered during the course of our audit.....	7
Disagreements with management.....	7
Any other significant matters	7
ACKNOWLEDGEMENTS	7
APPENDIX 1 – INTERNAL CONTROL MATTERS	8

REPORT TO THOSE CHARGED WITH GOVERNANCE

INTRODUCTION

1. We have completed our audit of the 31 December 2023 financial statements of the Office of the Commissioner of Police (the “Office” or “OCP”). International Standards on Auditing (ISAs) require that we communicate certain matters to those charged with governance of the Office in sufficient time to enable appropriate action. The matters we are required to communicate under ISAs include:
 - Auditors’ responsibilities in relation to the audit
 - the overall scope and approach to the audit, including any expected limitations, or additional requirements
 - relationships that may bear on our independence, and the integrity and objectivity of our staff
 - expected modifications to the audit report
 - significant findings from our audit.
2. This report sets out for the consideration of those charged with governance those matters arising from the audit of the financial statements that we consider are worthy of drawing to your attention.
3. This report has been prepared for the sole use of those charged with governance and we accept no responsibility for its use by a third party. Under the Freedom of Information Act (2020 Revision), it is the policy of the Office of the Auditor General to release all final reports proactively through our website: www.auditorgeneral.gov.ky.

AUDITOR’S RESPONSIBILITIES IN RELATION TO THE AUDIT

AUDITOR’S RESPONSIBILITY UNDER INTERNATIONAL STANDARDS ON AUDITING

4. ISAs require that we plan and perform the audit to obtain reasonable, rather than absolute, assurance about whether the financial statements are free of material misstatement. An audit of financial statements is not designed to identify all matters that may be relevant to those charged with governance. Accordingly, the audit does not ordinarily identify all such matters and this report

includes only those matters of interest which came to our attention as a result of the performance of our audit.

RESPONSIBILITIES OF MANAGEMENT AND THOSE CHARGED WITH GOVERNANCE

5. Management's responsibilities are detailed in the engagement letter signed by management on 13 September 2023 to which this engagement was subject. The audit of the financial statements does not relieve management or those charged with governance of their responsibilities.

OTHER INFORMATION IN DOCUMENTS CONTAINING AUDITED FINANCIAL STATEMENTS:

6. While we have no responsibility to perform any audit work on other information, including forward looking statements, containing audited financial statements, we will read the other information contained in the Office's annual report to consider whether such information is materially consistent with information appearing in the financial statements or our knowledge of the operations of the Office.

CONDUCT, APPROACH AND OVERALL SCOPE OF THE AUDIT

7. Information on the integrity and objectivity of the Office of the Auditor General and audit staff, and the nature and scope of the audit, were outlined in the Engagement Letter presented to the Chief Officer and follow the requirements of the ISAs. We are not aware of any impairment to our independence as auditors.

AUDIT REPORT, ADJUSTMENTS AND MANAGEMENT REPRESENTATION

8. We have issued an unmodified auditor's report on the 2023 financial statements.
9. There were no audit adjustments made to the financial statements.
10. As part of the completion of our audit we obtained written representations from management on aspects of the accounts and judgments and estimates made. These representations were provided to us on 15 March 2023.

SIGNIFICANT FINDINGS FROM THE AUDIT

SIGNIFICANT ACCOUNTING PRACTICES

11. We are responsible for providing our views about qualitative aspects of the Office's significant accounting practices, including accounting policies, accounting estimates and financial statement disclosures. Generally accepted accounting principles provide for the Office to make accounting estimates and judgments about accounting policies and financial statement disclosures.

We are, however, not aware of any new or controversial accounting practices reflected in the Office's financial statements.

MANAGEMENT'S JUDGMENTS AND ACCOUNTING ESTIMATES

12. OCP made a provision for legal liabilities in the amount of \$1.025m for the 2022 financial year.

GOING CONCERN DOUBTS

13. As a result of our audit, we did not become aware of any material uncertainties related to events and conditions that may cast significant doubt on the Office's ability to continue as a going concern.

SIGNIFICANT AND OTHER DEFICIENCIES IN INTERNAL CONTROL

14. We identified significant internal control deficiencies as part of our audit. Details of such deficiencies and other deficiencies (if any) are included in Appendix 1 along with management's response.

FRAUD OR ILLEGAL ACTS

15. Applicable auditing standards recognize that the primary responsibility for the prevention and detection of fraud and compliance with applicable acts and regulations rests with both those charged with governance of the entity and with management. It is important that management, with the oversight of those charged with governance; place a strong emphasis on fraud prevention and fraud deterrence. They are also responsible for establishing and maintaining controls pertaining to the Office's objective of preparing financial statements that are presented fairly, in all material respects, in accordance with the applicable financial reporting framework and managing risks that may give rise to material misstatements in those financial statements. In exercising oversight responsibility, those charged with governance should consider the potential for management override of controls or other inappropriate influence over the financial reporting process.

16. As auditors, in planning and performing the audit, we are required to reduce audit risk to an acceptably low level, including the risk of undetected misstatements in the financial statements due to fraud. However, we cannot obtain absolute assurance that material misstatements in the financial statements will be detected because of such factors as the use of judgment, the use of testing, the inherent limitations of internal control and the fact that much of the audit evidence available to the auditor is persuasive rather than conclusive in nature.

17. No fraud or illegal acts came to our attention as a result of our audit.

SIGNIFICANT DIFFICULTIES ENCOUNTERED DURING THE COURSE OF OUR AUDIT

18. No serious difficulties were encountered in the performance of our audit.

DISAGREEMENTS WITH MANAGEMENT

19. We have had no disagreements with management resulting from our audit.

ANY OTHER SIGNIFICANT MATTERS

20. There were no other significant matters noted during the audit other than those disclosed in Appendix 1.

ACKNOWLEDGEMENTS

21. We would like to express our thanks to the staff of the Office of the Commissioner of Police for their help and assistance during the audit of this year's financial statements. This enabled us to provide an audit report within the agreed timetable.

Yours sincerely,



Sue Winspear

Auditor General

APPENDIX 1 – INTERNAL CONTROL MATTERS

Observation	Risk/Implication and Recommendation	Management Response	Implementation Date
<p>1. Deficient controls over user rights</p> <p>We noted that the CSD staff who developed the application have administrative rights. A review of the user listing indicated that 4 CSD staff have Admin rights to the application. One of the CSD staff has access to all user groups. We further noted that two employees from OCP (inspector and administrative Secretary) also have full access to the application.</p> <p>Having developer, admin, input, and approval rights is a control deficiency, as a user can alter information input into the system without any due checks.</p>	<p>Risk/Implication: Granting developers, admins, input, and approval rights creates a control deficiency because it allows them to modify information without proper checks.</p> <p>Recommendation: Management should also review the application users and ensure that they only have the rights necessary to perform their roles.</p>	<p>Management accepts the recommendation regarding the Back-Office application.</p> <p>Management will work with the Computer Services Department (CSD) to document all classifications of users and the associated access rights for each classification.</p> <p>Each user will only be granted the access rights necessary to facilitate the successful performance of their role.</p> <p>Management will also request that Administrative, Approval and Input access rights currently held by CSD personnel be terminated, and the Admin roles be completed by OCP personnel only.</p>	<p>September 30, 2024</p>

Observation	Risk/Implication and Recommendation	Management Response	Implementation Date
<p>2. Delayed revocation of user access</p> <p>We noted that an ex-employee's access rights were revoked six months after he left OCP. A review of the leaver's schedule showed that the employee left on 28 July 2023, but communication to revoke and confirmation of revoking his access rights was sent on 31 January 2024.</p> <p>Delayed revoking of user access can lead to unauthorised access to information.</p>	<p>Risk/Implication:</p> <p>Delayed revoking of user access can lead to unauthorised access to information.</p> <p>Recommendation:</p> <p>Management should ensure prompt revocation of access once a user leaves the OCP.</p>	<p>This procedure has been formalized in the draft policy document. Refer to Observation #5.</p>	<p>September 15, 2024</p>
<p>3. High number of users with Admin rights</p> <p>We noted that 11 out of 22 PCC users have Admin rights, which gives them full access to the application.</p> <p>Unauthorised changes could be made to the application.</p>	<p>Risk/Implication:</p> <p>Unauthorized changes could be made to the application.</p> <p>Recommendation:</p> <p>Management should review the application users and ensure that they only have rights necessary to perform their roles.</p>	<p>Management will work with CSD to ensure only current employees retain access to the application.</p> <p>Management will document all classifications of users and the associated access rights for each classification.</p> <p>Each user will only be granted the access rights necessary to facilitate the successful performance of their role.</p>	<p>September 30, 2024</p>

Observation	Risk/Implication and Recommendation	Management Response	Implementation Date
<p>4. Deficient controls over adding new users</p> <p>During our review, we noticed that management did not communicate user rights when adding a new user. Specifically, when one employee was added, we observed that her user rights were not specified in the email sent to CSD/IT requesting her addition. The IT Administrator informed us that users are typically given basic access unless their specific access needs are communicated in the request. This particular employee was given cashier rights, which were not communicated in the request.</p> <p>There is a risk that a user could be granted access beyond what they need to perform their role.</p>	<p>Risk/Implication:</p> <p>There is a risk that a user could be granted access beyond what they need to perform their role.</p> <p>Recommendation:</p> <p>Management should ensure that the appropriate level of access is specified when requesting the addition of a new user.</p>	<p>An access request form will be developed, specifying the user type/level of access required, which must be approved by the Administrator. Each new user will only be granted the access rights necessary to facilitate the successful performance of their role.</p>	<p>September 30, 2024</p>
<p>5. Lack of a user manual for PCC online</p> <p>We noted that OCP had not created a user manual for PCC online, which would provide operational guidance and improve the consistency and continuity of operations.</p> <p>The absence of a user manual could result in a loss of application knowledge if current users depart without passing it on.</p>	<p>Risk/Implication:</p> <p>The absence of a user manual could result in a loss of application knowledge if current users depart without passing it on.</p> <p>Recommendation:</p> <p>Management should ensure that a user manual is developed to provide operational guidance and improve the consistency and continuity of operations.</p>	<p>A draft policy and procedure document has been developed. Once the user access classifications and access rights are finalized, the policy will be updated and submitted for final approval by the Chief Officer.</p>	<p>September 15, 2024</p>

