

The Honorable County Executive
The Honorable Members of the County Council
Anne Arundel County, Maryland
Annapolis, Maryland

In planning and performing our audit of the financial statements of Anne Arundel County, Maryland (the County), as of and for the year ended June 30, 2018, in accordance with auditing standards generally accepted in the United States of America, we considered the County's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the County's internal control. Accordingly, we do not express an opinion on the effectiveness of the County's internal control. Our report includes a reference to other auditors who audited the financial statements of Tipton Airport Authority and the Anne Arundel Workforce Development Corporation as described in our report on the County's financial statements. The County's financial statements also include the Anne Arundel Community College, the Anne Arundel Board of Education and the Anne Arundel Economic Development Corporation which were separately audited by us. This report does not include the results of our and the other auditors' testing of internal controls over financial reporting or compliance and other matters for the Anne Arundel County Board of Education, Anne Arundel Community College, the Anne Arundel Economic Development Corporation, Tipton Airport Authority, and Anne Arundel Workforce Development Corporation that are reported on separately by us and the other auditors.

However, during our audit we became aware of deficiencies in internal control other than significant deficiencies and material weaknesses and other matters that are opportunities to strengthen your internal control and improve the efficiency of your operations. Our comments and suggestions regarding these matters are summarized below. This letter does not affect our report on the financial statements dated December 21, 2018, nor our internal control communication dated December 21, 2018.

DEPARTMENT OF PUBLIC WORKS

Monitoring of Financial Data

Significant financial data is prepared or compiled by departments other than the Office of Finance. Currently, the Department of Public Works (DPW) tracks revenues, unearned revenues, and related receivables using complex spreadsheets with large amounts of information (project file listing). The accuracy of the information in the project file listing is imperative in determining when revenues, unearned revenues, and related receivables should be recognized and reported to the Office of Finance. The DPW uses an established checklist to determine that all necessary year-end closing procedures are complete. Currently, many of these closing procedures are performed manually due to the lack of automated processes in place over the project file listing. Such a lack of automated controls increases the possibility of human error during the year end closing process. Management should

investigate automating all or part of this process in order to lower the risk related to the manual process. Additionally, management should periodically review procedures included in the year-end checklist to ensure that the procedures include reviews of all information that could potentially impact the project file listing.

Management's Response:

DPW has been working with OIT for approximately two years to implement the development of an automated Utility Allocation Tracking and Billing software system. The new system will address the numerous and complicated financial requirements related to project development and will provide automated reporting for the year-end closing. The new system is running simultaneously with our current system. The testing should be completed by the end of this fiscal year.

The Office of Finance and DPW will continue to work closely together to make sure that accounts are properly recorded.

OFFICE OF FINANCE

Reconciliation and Recording of Impact Fees Revenue

The County completes a reconciliation of impact fees from the PIPS (Permit Information Processing System) system prior to recording the revenue in EnterpriseOne. The reconciliation process is performed using reports from the PIPS system. We noted that the reconciliations contained numerous reconciling items between the PIPS reports and the general ledger. CLA found two instances where revenue transactions included in the reconciliation as reconciling items did not agree with cash receipts.

We were able to review the cash receipts and verify that the revenue was recorded properly in EnterpriseOne, therefore the financial statements were correct. However, improper inclusion of such items on the reconciliation could lead to difficulties in the reconciliation process. We recommend management review its policies and procedures for the reconciliation of impact fees per PIPS to the general ledger.

Management's Response:

There was a problem with the reports needed to perform the reconciliation. The original reports needed to be revised to expand the date range related to the permits. The original reports did not include a permit if the date of the permit was outside of the month being reconciled. OIT has updated the report criteria which has corrected this issue. The updated report shows all activity related to the permits. Finance is able to identify the items that relate to the current month being reconciled, therefore, no items are being missed on the tracking sheets. This has simplified the reconciliation process.

OFFICE OF INFORMATION TECHNOLOGY

Information Technology

We noted several items in information technology policies and procedures that merit management's attention. These items are not individually significant; however, without corrective action these items could increase the County's system vulnerability.

- There were two instances noted during our testing in which access for terminated employees was not properly removed. These instances are noted below:
 - A Deletion of Network Access request for one Office of Finance employee was not submitted until 4 months after termination and OIT Help Desk was not otherwise notified of the employee's termination. The user was on maternity leave prior to voluntary termination. The user had access to a financial application. The County's current policy requires submission of a Deletion of Network Access request in the automated ticketing system, by the technical coordinator of the terminated employee's department, upon termination. The user's accounts were not flagged for inactivity and action to remove the user's account was not taken until the User Recertification in August.
 - A Deletion of Network Access request for one Office of Finance employee was not submitted until 4 months after termination and OIT Help Desk was not otherwise notified of the employee's termination. The user retired in April and was rehired in November. The user had access to the network, a financial application, and was a VPN user. The County's current policy requires submission of a Deletion of Network Access request in the automated ticketing system, by the technical coordinator of the terminated employee's department, upon termination. The user's accounts were not flagged for inactivity and action to remove the user's account was not taken until the User Recertification in August.

We recommend that the Office of Information Technology implement a system control to disable accounts after a period of inactivity. This will limit unauthorized access to unmonitored accounts and reduce the possibility of enabled accounts for terminated users that OIT was not made aware of by the user's department.

- OIT has not conducted an IT Risk Assessment since 2015 and is working through the findings from that assessment. Additionally, an external penetration test has not been conducted in the past 3 years.

We recommend that the Office of Information Technology conduct an IT Risk Assessment to address the current status of the County's network and system. Additionally, an external penetration test should be conducted to determine what vulnerabilities exist as a result of technology and industry changes since 2015.

Management's Response:

The Office of Information Technology has acknowledged the recommendations of the auditor and are reviewing our policy concerning inactivity and considering our options. Currently, we have multiple vendors that require uninterrupted access to internal servers. These support accounts may not remote

in for several months and an inactivity timer could adversely impact our ability to restore a system in the event of a failure.

The Finance Office Department Manager (or supervisor in the manager’s absence) will notify the department administrators of the employee’s departure (resignation, termination, retirement, transfer etc.). They will submit the user deletion request through OIT’s Heat system and confirm timely processed as requested.

In reference to the second finding recommending a risk assessment and penetration test, the Office of Information Technology has taken steps to have third-party vendors perform risk assessments on high-risk areas of our network. In 2018, the vendor, SADA, conducted a risk assessment of the County’s G Suite Services (i.e., Google Mail, Drive, etc.) and Mission Critical Partners conducted a risk assessment of our public safety environment. We are also submitting paperwork to the Department of Homeland Security to perform penetration tests of our network as soon as possible.

PRIOR YEAR COMMENTS

The following table reflects previous internal control communications that are currently in process and have not been fully corrected. We recommend that management implement those recommendations where no progress has been made to date.

Recommendation	Year of Origination
1. Management should review the subsidiary records for escrow deposits in the Reforestation Fund, and return the deposits or take the deposits into County revenue as appropriate.	2009
2. Management should review the password setting for all County systems to ensure that they are appropriate and in accordance with County policies. Minimum password length for a financial and reporting system used by the County do not conform to County Information Technology Security policies. This increases the risk of unauthorized access to the organization’s financially significant systems and data.	2012
3. Flash drives issued to County staff should be encrypted.	2016
4. USB ports on County staff hardware/systems should be locked.	2016
5. Management should determine one single department that oversees the entire utility billing process.	2016
6. The County’s repurchase agreements were not fully collateralized at year end. We recommend management review its policies and procedures for monitoring collateral requirements with banks holding repurchase agreements for the County to ensure accounts are properly collateralized at all times.	2017

Management's Response:

- 1) Review of escrow deposit subsidiary records for the Reforestation Fund is continuing. To ensure resolution, the department has made this program part their Performance Indicators in FY2016 and beyond, and has pursued contractual employee assistance in completing this process. In fiscal year 2018 the escrow balance decreased from \$5,802,860 at July 1, 2017 to \$5,454,944 on June 30, 2018, a \$347,916 decrease. The total balance of escrow deposits from 2009 and earlier years has also dropped from \$1,781,929 on June 30, 2017 to \$1,596,108 on June 30, 2018, a decrease of \$185,821 or 10% for years 2009 and earlier. The Office of Inspections & Permits continues to work on clearing the backlog and has cleared an additional 20% since the fiscal year-end. For FY19 the County (I&P) budgeted approx. \$2.0 million to be sent the Chesapeake Bay Trust (CBT) for planting in FY19.
- 2) Management has enacted a best practices policy over password settings and reviewed County systems to put them into compliance with that policy. At the time of the audit, EnterpriseOne was not capable of supporting the password complexity requirements necessary to adhere to the OIT Security policy. In 2018, there was an upgrade to the system which provided support for password complexity. Management is in the process of reviewing the impacts of the change and will be following internal processes to test and deploy the change.
- 3) &
- 4) Management has reviewed the risk of permitting unencrypted flash drives and unlocked USB ports throughout the organization and has decided to accept the risk. The cost of implementing an enterprise solution and the resources requirement to manage it is cost prohibitive and could adversely impact a department's ability to meet their business objectives. Where there is an increased risk of the loss of sensitive data (e.g., laptops), Management will be implementing a security solution that encrypts hard drives and USB ports and recommending the department's data custodian implement processes and procedures to ensure sensitive data is not stored on unencrypted drives. The Health Department has implemented the security solution on all of their laptops in 2018 and OIT is currently testing it on laptops. Additionally, Management has rolled out security awareness training to educate users on how to protect data from loss or theft.
- 5) The Office of Information Technology has searched for an information technology system that can address the entire utility billing process, but discovered no one system that can accomplish all of the tasks involved. No one vendor makes a product that covers the process from reading meters to printing the related bills. Until that exists, we will have multiple systems that accomplish this task.
- 6) The County's investment policy includes the sentence "Margin calls are initiated when repo collateral falls under 101% or is \$100,000 less than the required 102% level." The collateralization level of 101.9%, as calculated by audit, is greater than 101% and therefore within the investment policy requirement.

The following table reflects previous internal control communications that have been fully implemented/corrected during the current year.

Recommendation	Year of Origination
1. Formal requests for system changes should be through a ticket tracking system. This system should track the requester, approver, reviewer, dates, and at which stage the request resides.	2016

* * * *

We will review the status of these comments during our next audit engagement. We have already discussed many of these comments and suggestions with various County personnel, and we thank the personnel of the County for their courteous cooperation. We would be pleased to discuss them in further detail at your convenience, to perform any additional study of these matters, or to assist you in implementing the recommendations.

Management's written responses to the matters noted above have not been subjected to the auditing procedures applied in the audit of the County's basic financial statements and, accordingly, we express no opinion on management's responses.

This communication is intended solely for the information and use of the County Executive, County Council, management, and federal awarding agencies and pass-through entities and is not intended to be, and should not be, used by anyone other than these specified parties.



CliftonLarsonAllen LLP

Baltimore, Maryland
December 21, 2018