



VIRGINIA CORRECTIONAL ENTERPRISES

INTERNAL CONTROL QUESTIONNAIRE

REVIEW RESULTS

AS OF

JUNE 2020

Auditor of Public Accounts
Martha S. Mavredes, CPA
www.apa.virginia.gov
(804) 225-3350



- TABLE OF CONTENTS -

	<u>Pages</u>
REVIEW LETTER	1-4
AGENCY RESPONSE	5-9



Martha S. Mavredes, CPA
Auditor of Public Accounts

Commonwealth of Virginia

Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

August 11, 2020

Marie Vargo, Chief Executive Officer
Virginia Correctional Enterprises
8030 Whitebark Terrace
Richmond, VA 23237

INTERNAL CONTROL QUESTIONNAIRE REVIEW RESULTS

We have reviewed the Internal Control Questionnaire for **Virginia Correctional Enterprises** (Correctional Enterprises). We completed the review on June 12, 2020. The purpose of this review was to evaluate if the agency has developed adequate internal controls over significant organizational areas and activities and not to express an opinion on the effectiveness of internal controls. Management of Correctional Enterprises is responsible for establishing and maintaining an effective control environment.

The Auditor of Public Accounts has developed a new process for auditing agencies that are not required to have an audit every year, which we refer to as "cycled agencies." Traditionally, we audit these agencies at least once every three years. We now employ a risk-based approach to auditing the cycled agencies. Under this approach, annually we will perform a risk analysis for all of the cycled agencies considering certain criteria and divide the agencies into two pools. One pool will receive an annual audit and the other pool will be subject to review in a special project focused on one area of significance as well as a review of internal controls in the form of a questionnaire. Our intent is that all cycled agencies will complete an internal control questionnaire at least once every three years. This letter is to communicate the results of the Internal Control Questionnaire review.

Review Process

During the review, the agency completes an Internal Control Questionnaire that covers significant organizational areas and activities including payroll and human resources; revenues and expenses; procurement and contract management; capital assets; grants management; debt; and information technology and security. The questionnaire focuses on key controls over these areas and activities.

We review the agency responses and supporting documentation to determine the nature, timing, and extent of additional procedures. The nature, timing, and extent of the procedures selected depend on our judgment in assessing the likelihood that the controls may fail to prevent and/or detect events that could prevent the achievement of the control objectives. The procedures performed target risks or business functions deemed significant and involve reviewing internal policies and procedures. Depending on the results of our initial procedures, we may perform additional procedures including reviewing evidence to ascertain that select transactions are executed in accordance with the policies and procedures and conducting inquiries with management. The “Review Procedures” section below details the procedures performed for Correctional Enterprises. The results of this review will be included within our risk analysis process for the upcoming year in determining which agencies we will audit.

Review Procedures

We evaluated the agency’s corrective action for the finding from the fiscal year 2015 audit. We determined that although some progress has been made, corrective action is not complete and this finding is repeated in the “Review Results” section below. Due to the implementation of the new statewide accounting system, we reviewed a selection of system and transaction reconciliations in order to gain assurance that the statewide accounting system contains accurate data. Further, we evaluated the agency’s process of completing and submitting attachments to Department of Accounts (Accounts).

We reviewed the Internal Control Questionnaire and supporting documentation detailing policies and procedures. As a result of our review, we performed additional procedures over the following areas: payroll and human resources; revenues and expenses; contracts management; capital assets; and information systems security. These procedures included validating the existence of certain transactions; observing controls to determine if the controls are designed and implemented; reviewing transactions for compliance with internal and Commonwealth policies and procedures; and conducting further review over management’s risk assessment process.

As a result of these procedures, we noted areas that require management’s attention. These areas are detailed in the “Review Results” section below.

Review Results

We noted the following areas requiring management’s attention resulting from our review:

- Correctional Enterprises does not maintain its own specific and up-to-date policies and procedures for all business areas that are not covered by the Department of Corrections’ (Corrections) policies. During our review, we noted the following items related to the documentation of Correctional Enterprises’ policies and procedures:
 - There are no internal policies and procedures for several key processes including the preparation and review of attachments sent to Accounts; the preparation, review, and

reconciliation of payroll data sent to Corrections' Payroll Department; or the confirmation of information submitted to the Virginia Retirement System.

- Correctional Enterprises' existing policies do not include key controls such as periodic system access reviews for its enterprise resource planning system or the review of system logs and audit trails.

Topic 20905 and other sections of the Commonwealth Accounting Policies and Procedures (CAPP) Manual state that each agency must, "publish its own policies and procedures documents, approved in writing by agency management." Correctional Enterprises should establish formal, documented procedures over all critical business processes not already covered by Corrections' policies, have management approve the procedures, and update them regularly in order to maintain an effective control environment.

- Correctional Enterprises could not provide evidence that it reconciled the human resources system to the retirement benefits system prior to confirming the accuracy of information in the retirement system for one of two months selected. Topic 50410 of the CAPP Manual states that agencies should reconcile data from the human resources system to the retirement system at the beginning of each month.
- **Partial Repeat** - Correctional Enterprises removed information systems access for a separated employee four days after the individual's last day of employment. The Commonwealth's Information Security Standard, SEC 501, (Security Standard), Section PP4, requires the disabling of information systems access within 24 hours of the employee's last day. Correctional Enterprises' system access policy requires removal of systems access for separating employees no later than 30 days after their separation, which is not in agreement with the Security Standard. Correctional Enterprises should update its policy to be in alignment with the Security Standard and should ensure system access is disabled for separating employees within 24 hours of their last day of employment.
- Correctional Enterprises could not provide evidence of its most recent systems access review. Section AC-6 of the Security Standard requires the organization to review on an annual basis the privileges assigned to all users to validate the need for such privileges. Correctional Enterprises should conduct and document such a review in sufficient detail on an annual basis.
- For Correctional Enterprises' internal systems, there is not an automatic disabling of accounts not used for extended periods of time. Section AC-2-COV of the Security Standard states that agencies should disable unneeded accounts in a timely manner. Correctional Enterprises should implement an automatic disabling of access after an extended period of inactivity. Or, if such a control is not possible, Correctional Enterprises should review accounts for inactivity and manually disable unneeded accounts.

- Correctional Enterprises does not regularly review system logs or other system audit documentation; instead, reviews are currently only performed when there is a known or suspected issue. Section AU-6 of the Security Standard requires the organization to review information security records at least every 30 days for indications of inappropriate or unusual activity and report any findings to designated organizational officials. Correctional Enterprises should conduct regular reviews of system audit documentation for its enterprise resource planning system to ensure an effective control environment.
- Correctional Enterprises' system administrators are responsible for reviewing system administrator activity in the enterprise resource planning system. Section AC-5 of the Security Standard requires the organization to separate the duties of individuals as necessary to prevent malevolent activity. Correctional Enterprises should ensure that an individual with no system administrator responsibilities is responsible for reviewing system administrator activities.
- Correctional Enterprises does not have an adequately documented contingency plan in place. Section CP-1 of the Security Standard lays out the requirements for all agencies' contingency planning documents. Correctional Enterprises should develop contingency planning documents to address each item identified in the Security Standard to ensure compliance.

We discussed these matters with management on July 20, 2020. Management's response to the findings identified in our review is included in the section titled "Agency Response." We did not validate management's response and, accordingly, cannot take a position on whether or not it adequately addresses the issues in this report.

This report is intended for the information and use of management. However, it is a public record and its distribution is not limited.

Sincerely,

Martha S. Mavredes
Auditor of Public Accounts

JDE\vks



COMMONWEALTH of VIRGINIA

Department of Corrections

Virginia Correctional Enterprises

Headquarters: 804-743-4100
Customer Service: 800-823-2823

8030 White Bark Terrace
North Chesterfield, VA 23237

August 27, 2020

Ms. Martha Mavredes
Auditor of Public Accounts
P.O. Box 1295
Richmond, VA 23218

RE: Internal Control Questionnaire Review Results

Virginia Correctional Enterprises (VCE) has reviewed the Auditor of Public Accounts (APA) Internal Control Questionnaire Review Results. Please find management's response and action plan, below.

Summarization of Audit Finding:

Correctional Enterprises does not maintain its own specific and up-to-date policies and procedures for all business areas which are not covered by the Department of Corrections' (Corrections) policies. During our review, we noted the following items related to the documentation of Correctional Enterprises' policies and procedures:

- There were no internal policies and procedures for several key processes including the preparation and review of attachments sent to Accounts; the preparation, review, and reconciliation of payroll data sent to Corrections' Payroll Department; or the confirmation of information submitted to the Virginia Retirement System.
- Correctional Enterprises' existing policies do not include key controls such as periodic system access reviews for its enterprise resource planning system or the review of system logs and audit trails.

Topic 20905 and other sections of the Commonwealth Accounting Policies and Procedures (CAPP) Manual state that each agency must, "publish its own policies and procedures documents, approved in writing by agency management." Correctional Enterprises should establish formal, documented procedures over all critical business processes not already covered by Corrections' policies, have management approve the procedures, and update them



regularly in order to maintain an effective control environment.

VCE Corrective Action Plan:

In response to the APA finding, Management concurs. VCE's Business Manager will prepare a procedure that documents the process to complete financial attachments due to the Department of Accounts.

During FY2020, the VCE transferred its IT and HR positions to fall under the direct supervision of the Department of Corrections (DOC). VCE will work with DOC to review existing procedures and prepare additional, VCE specific sections.

Target Date for Completion:

The fiscal procedure will be completed by September 30, 2020.

The HR and IT procedures specific to VCE will be completed by December 31, 2020.

Responsible Person/Positions:

VCE's Business Manager will complete the fiscal procedure.

VCE's assigned HR Supervisor will be responsible for reviewing and updating the HR procedure.

VCE's Information Systems Manager will be responsible for reviewing and updating the IT procedure.

Summarization of Audit Finding:

Correctional Enterprises could not provide evidence that it reconciled the human resources system to the retirement benefits system prior to confirming the accuracy of information in the retirement system for one of two months selected. Topic 50410 of the CAPP Manual states that agencies should reconcile data from the human resources system to the retirement system at the beginning of each month.

VCE Corrective Action Plan:

In response to the APA finding, Management concurs. The month that the reconciliation could not be found was performed by an employee no longer at VCE. The current staff are aware of the requirements. No further action is deemed necessary.

Target Date for Completion:

The requirement is completed

Responsible Person/Positions:

VCE's assigned HR Supervisor will ensure the reconciliations are performed according to policy.

Summarization of Audit Finding:

Correctional Enterprises removed information systems access for a separated employee four days after the individual's last day of employment. The Commonwealth's Information Security Standard, SEC 501, (Security Standard), Section PP4 requires the disabling of information systems access within 24 hours of the employee's last day. Correctional Enterprises' system access policy requires removal of systems access for separating employees no later than 30 days after their

separation which is not in agreement with the Security Standard. Correctional Enterprises should update its policy to be in alignment with the Security Standard and should ensure system access is disabled for separating employees within 24 hours of their last day of employment.

VCE Corrective Action Plan:

During FY2020, the VCE transferred its IT and HR positions to fall under the direct supervision of the Department of Corrections (DOC). VCE will work with DOC to review existing procedures and prepare additional, VCE specific sections.

Target Date for Completion:

The procedure will be updated by December 31, 2020. The initial audit of active accounts to the personnel roster has been completed and will be repeated at regular intervals.

Responsible Person/Positions:

VCE's Information Systems Manager and Human Resources Supervisor will be responsible for updating this procedure to ensure user accounts are deleted on a timely basis.

Summarization of Audit Finding:

Correctional Enterprises could not provide evidence of its most recent systems access review. Section AC-6 of the Security Standard requires the organization review on an annual basis the privileges assigned to all users to validate the need for such privileges. Enterprises should conduct and document such a review in sufficient detail on an annual basis.

VCE Corrective Action Plan:

During FY2020, the VCE transferred its IT and HR positions to fall under the direct supervision of the Department of Corrections (DOC). VCE will work with DOC to review existing procedures and prepare additional, VCE specific sections.

Target Date for Completion:

The procedure will be updated by December 31, 2020.

Responsible Person/Positions:

VCE's Information Systems Manager will be responsible for reviewing and updating the procedure.

Summarization of Audit Finding:

For Correctional Enterprises' internal systems, there is not an automatic disabling of accounts not used for extended periods of time. Section AC-2-COV of the Security Standard states that agencies should disable unneeded accounts in a timely manner. Correctional Enterprises should implement an automatic disabling of access after an extended period of inactivity. Or, if such a control is not possible, Correctional Enterprises should review accounts for inactivity and manually disable unneeded accounts.

VCE Corrective Action Plan:

During FY2020, the VCE transferred its IT and HR positions to fall under the direct supervision of the Department of Corrections (DOC). VCE will work with DOC to review existing procedures and prepare additional, VCE specific sections.

Target Date for Completion:

The procedure will be updated by December 31, 2020.

Responsible Person/Positions:

VCE's Information Systems Manager will be responsible for reviewing and updating the procedure.

Summarization of Audit Finding:

Correctional Enterprises does not regularly review system logs or other system audit documentation; instead, reviews are currently only performed when there is a known or suspected issue. Section AU-6 of the Security Standard requires the organization to review information security records at least every 30 days for indications of inappropriate or unusual activity and report any findings to designated organizational officials. Correctional Enterprises should conduct regular reviews of system audit documentation for its enterprise resource planning system to ensure an effective control environment.

VCE Corrective Action Plan:

During FY2020, the VCE transferred its IT and HR positions to fall under the direct supervision of the Department of Corrections (DOC). VCE will work with DOC to review existing procedures and prepare additional, VCE specific sections.

Target Date for Completion:

The procedure will be updated by December 31, 2020.

Responsible Person/Positions:

VCE's Information Systems Manager will be responsible for reviewing and updating the procedure.

Summarization of Audit Finding:

Correctional Enterprises' system administrators are responsible for reviewing system administrator activity in the enterprise resource planning system. Section AC-5 of the Security Standard requires the organization to separate the duties of individuals as necessary to prevent malevolent activity. Correctional Enterprises should ensure that an individual with no system administrator responsibilities is responsible for reviewing system administrator activities.

VCE Corrective Action Plan:

During FY2020, the VCE transferred its IT and HR positions to fall under the direct supervision of the Department of Corrections (DOC). VCE will work with DOC to review existing procedures and prepare additional, VCE specific sections.

Target Date for Completion:

The procedure will be updated by December 31, 2020.

Responsible Person/Positions:

VCE's Information Systems Manager will be responsible for reviewing and updating the procedure.

Summarization of Audit Finding:

Correctional Enterprises does not have an adequately documented contingency plan in place. Section CP-1 of the Security Standard lays out the requirements for all agencies' contingency planning documents. Correctional Enterprises should develop contingency planning documents to address each item identified in the Security Standard to ensure compliance.

VCE Corrective Action Plan:

During FY2020, the VCE transferred its IT and HR positions to fall under the direct supervision of the Department of Corrections (DOC). VCE will work with DOC to review existing procedures and prepare additional, VCE specific sections.

Target Date for Completion:

The procedure will be updated by December 31, 2020.

Responsible Person/Positions:

VCE's Information Systems Manager will be responsible for reviewing and updating the procedure.

Please let me know if you have any questions regarding this response.

Sincerely,

A handwritten signature in blue ink, appearing to read 'Marie Vargo', is written over a printed name.

Marie Vargo
VCE Chief Executive Officer