



DEPARTMENT OF ENVIRONMENTAL QUALITY

INTERNAL CONTROL QUESTIONNAIRE REVIEW RESULTS AS OF JULY 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	5-7



Martha S. Mavredes, CPA
Auditor of Public Accounts

Commonwealth of Virginia

Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

August 18, 2020

David Paylor
Department of Environmental Quality
P.O. Box 1105
Richmond, VA 23218

INTERNAL CONTROL QUESTIONNAIRE REVIEW RESULTS

We have reviewed the Internal Control Questionnaire for **Department of Environmental Quality** (Environmental Quality). We completed the review on July 2, 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 Environmental Quality is responsible for establishing and maintaining an effective control environment.

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 Environmental Quality. 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 prior review finding. We determined that although significant progress has been made, corrective action is not fully complete and this finding is repeated in the "Review Results" section below.

We reviewed a selection of system and transaction reconciliations in order to gain assurance that the statewide accounting system contains accurate data. The definitive source for internal control in the Commonwealth is the Agency Risk Management and Internal Control Standards (ARMICS) issued by the Department of Accounts (Accounts); therefore, we also included a review of ARMICS. The level of ARMICS review performed was based on judgment and the risk assessment at each agency. At some agencies only inquiry was necessary; while others included an in-depth analysis of the quality of the Stage 1 Agency-Level Internal Control Assessment Guide, or Stage 2 Process or Transaction-Level Control Assessment ARMICS processes. Our review of the Environmental Quality's ARMICS program included a review of all current ARMICS documentation and a comparison to statewide guidelines established by Accounts. Further, we evaluated the agency's process of completing and submitting attachments to 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; procurement and contract management; capital assets; grants management; 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:

- **Partial Repeat** (with significant progress) - Environmental Quality should continue to make progress to address the findings related to information technology and security that were identified as a result of the information systems audit conducted by the Virginia Information Technologies Agency in March 2017. The audit identified and communicated 57 findings to management. Environmental Quality has marked 49 findings as complete, and eight as underway. Environmental Quality should continue to devote resources to addressing these recommendations and ensuring it is in compliance with the Commonwealth's Information Security Standard, SEC 501 (Security Standard).

- Environmental Quality does not have a sufficient process or formal policy for gaining assurance that third-party financial and information technology service providers have adequate controls in place. The Security Standard, Section 1.1, states that agency heads remain accountable for maintaining compliance with the Security Standard for information technology equipment, systems, and services procured from providers, and agencies must enforce the compliance requirements through documented agreements and oversight of the services provided. Additionally, Commonwealth Accounting Policies and Procedures (CAPP) Manual Topic 10305 requires agencies to have adequate interaction with providers to appropriately understand the providers' internal control environment. System and Organization Controls Reports (SOC reports) provide an independent description and evaluation of the provider's internal controls, but Environmental Quality does not have a formal process or policy for obtaining, reviewing and documenting SOC reports. Environmental Quality has not reviewed the SOC report for two service providers because there is no formal review process in place.

The lack of review over SOC reports limits Environmental Quality from ensuring that providers' controls are designed, implemented, and operating effectively. Environmental Quality should develop and implement policies and procedures to obtain SOC reports, review and assess the results, and document the effectiveness of provider controls reported through SOC reports. If the SOC report details complementary controls, Environmental Quality should ensure that these controls are documented and implemented at the agency. If control deficiencies are identified in SOC reports, Environmental Quality should determine if additional controls can be implemented at the agency to mitigate the risk until the provider corrects the deficiency.

- Environmental Quality does not meet the minimum requirements of ARMICS. Although Environmental Quality completed its agency-wide risk assessments, the agency did not document and test all key agency-level controls, transaction-level controls, or key elements of the control environment. CAPP Manual Topic 10305 requires agencies to document, evaluate, and test all agency-level and transaction-level controls to assess each element of the control environment. Further, there was not sufficient evidence to support that Environmental Quality documented and assessed how the agency gathers, uses, and disseminates information or monitors the effectiveness of agency internal controls. Environmental Quality should ensure compliance with the ARMICS minimum requirements.

- Environmental Quality lacks certain components of an established disaster recovery plan (DRP) in accordance with the Security Standard. The Security Standard, Section CP1-COV-2, requires Environmental Quality to develop and maintain a DRP that supports the restoration of mission essential functions and dependent business functions. The Security Standard, Section CP-1-COV-2, also requires that Environmental Quality periodically review, reassess, test, and revise the DRP to reflect changes in the mission essential functions, services, IT system hardware and software, and personnel. Environmental Quality does not currently have a DRP in place that supports the full restoration of systems, detailing the step-by-step processes and scripts required to be performed in the event of a disaster.

By not having a current, detailed DRP, Environmental Quality increases the risk of mission critical systems being unavailable to support essential services. In addition, by not performing annual tests against the DRP, Environmental Quality is unable to identify weaknesses in the plans and may unnecessarily delay the availability of sensitive systems in the event of a disaster or outage. Environmental Quality should develop a detailed DRP and perform annual tests against the DRP to ensure the agency can restore mission critical and sensitive systems in a timely manner in the event of an outage or disaster. Doing this will help to ensure Environmental Quality maintains the confidentiality, integrity, and availability of their mission critical and sensitive systems.

We discussed these matters with management on August 7, 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\clj



Commonwealth of Virginia

VIRGINIA DEPARTMENT OF ENVIRONMENTAL QUALITY

1111 E. Main Street, Suite 1400, Richmond, Virginia 23219

P.O. Box 1105, Richmond, Virginia 23218

(800) 592-5482

www.deq.virginia.gov

Matthew J. Strickler
Secretary of Natural Resources

David K. Paylor
Director
(804) 698-4000

August 31, 2020

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

Dear Ms. Mavredes:

This letter is in response to the recent audit of the Department of Environmental Quality (DEQ) for the period ending June 30, 2019, and the Internal Control Questionnaire Review Results letter received from APA. DEQ would like to provide responses to the following areas covered in your review.

Information Systems Audit:

APA's audit of March 2017 noted 57 findings related to information technology and security audit. DEQ has performed correction action to remediate 49 items but is continuing to work on the remaining eight findings.

Third Party Service Providers:

DEQ has a formal agreement with Elavon to handle credit card transactions for training courses. Prior to this year, DEQ had not requested a copy of the System and Organization Controls Report (SOC report) for Elavon from State Treasury. DEQ both recognizes and understands the need to request and review this report annually. DEQ has already requested, in writing, the SOC report from Treasury for FY 2020. This request will be ongoing at the conclusion of each fiscal year.

DEQ's third party service contract with Agilaire requires a subscription to the VITA Enterprise Cloud Oversight Service (ECOS). The ECOS team is responsible for monitoring the vendor's performance and ensuring that the vendor maintains compliance with COV policies. Part of their initial review (performed less than a year ago) included a review of the SOC report that Agilaire provided as well as the performance of a GAP analysis, which was completed/provided in December. In addition, DEQ will begin requesting and reviewing the SOC report for Agilaire annually to ensure that proper oversight is maintained and is kept aware of any complementary controls that should be in place or control deficiencies that should be addressed.

DEQ will also assess the SOC reports and document the effectiveness of the provider controls as reported in the SOC reports. If the SOC report details complementary controls, DEQ will ensure that these controls are documented and implemented at the agency. If control deficiencies are identified in SOC reports, DEQ will determine if additional controls can be implemented at the agency to mitigate the risk until the provider corrects the deficiency. The Fiscal Director will alert DEQ's management to any concerns. DEQ is currently writing a procedure outlining this handling of third party provider agreements.

Agency Risk Management and Internal Control Standards (ARMICS)

DEQ has done testing on the following transaction level processes in previous years: accounts payable, accounts receivable, fixed assets, procurement and various Human Resources (HR) policies. Those processes and controls that are deemed significant at the agency and transactional level will be documented and tested for FY 2020 prior to September 30, 2020. DEQ will make sure to document how the agency monitors the effectiveness of internal controls. DEQ will ensure documentation (by signature) of who completed the testing and documentation (by signature) for the reviewer of the testing. Additional significant processes to be incorporated in ARMICS testing for the September 30, 2020, certification include: Financial Reporting, Reconciliations, Federal grants and additional HR/payroll testing.

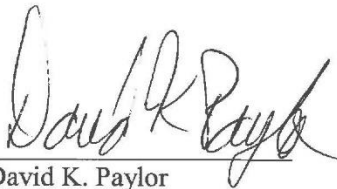
Information System Security

While DEQ concurs with the comments noting that we do not currently possess a detailed, step-by-step disaster recovery plan, DEQ does currently maintain detailed system configuration documentation that contains up-to-date information including hardware details, software version(s) and location information, key personnel/responsibility identification and application-specific configuration and backup information. While not formatted as a step-by-step disaster recovery playbook, this documentation is, in effect, the detailed documentation necessary to rebuild each of our core applications from the ground up. Additionally, mission essential functions are documented in the agency Continuity of Operations Plan, which is reviewed, updated and exercised annually. Going forward, DEQ will engage the necessary resources to enhance our recovery-related documentation and procedures as well as to identify and document processes for periodic testing and validation of those procedures.

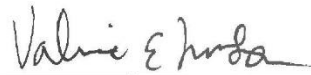
Auditor of Public Accounts
August 31, 2020

DEQ remains committed to meeting all requirements outlined in the APA's result letter. In addition, DEQ will assign staff to accomplish the noted matters. Please feel free to contact us if we can provide additional information.

Sincerely,



David K. Paylor
Agency Director



Valerie E. Thomson
Director of Administration