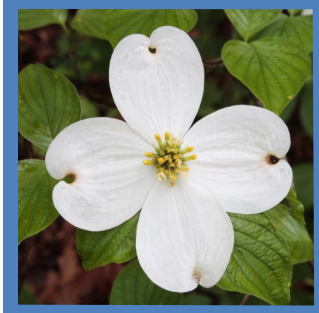


DEPARTMENT OF PROFESSIONAL AND OCCUPATIONAL REGULATION

INTERNAL CONTROL QUESTIONNAIRE REVIEW RESULTS AS OF AUGUST 2024

Auditor of Public Accounts
Staci A. Henshaw, CPA
www.apa.virginia.gov
(804) 225-3350

- TABLE OF CONTENTS -

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

September 4, 2024

Brian Wolford, Director
Department of Professional and Occupational Regulation
9960 Mayland Drive
Richmond VA 23233-1485

INTERNAL CONTROL QUESTIONNAIRE REVIEW RESULTS

We have reviewed the Internal Control Questionnaire for the **Department of Professional and Occupational Regulation** (Professional and Occupational Regulation). We completed the review on August 2, 2024. 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 Professional and Occupational Regulation 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 Professional and Occupational Regulation. 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 2021 internal control questionnaire review findings as well as the findings in the report titled "Cycled Agency Information Systems Security Review for the year ended June 30, 2019." The agency has taken adequate corrective action with respect to findings reported in the prior review and audits that are not 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 Professional and Occupational Regulation. Our review of Professional and Occupational Regulation's ARMICS program included a review of all current ARMICS documentation and a comparison to statewide guidelines established by Accounts. Further, we evaluated Professional and Occupational Regulation'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; and information technology and security. These procedures included validating the existence of certain transactions; observing controls to determine if the controls are effectively 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:

- **Repeat** – Professional and Occupational Regulation continues to not have adequate controls over audit logging and monitoring as required by the Commonwealth's Information Security Standard, SEC530 (Security Standard). Specifically, Professional and Occupational Regulation does not enable logs for three out of four sensitive systems. Professional and Occupational Regulation should ensure its sensitive systems record audit logs according to the Security Standard and should develop and implement a process to retain sensitive system audit logs and review at least every 30 days.

- **Repeat** – Professional and Occupational Regulation has formal, documented policies and procedures over many of its significant business processes. However, during our review, we

identified several critical business areas where Professional and Occupational Regulation should develop or improve policies and procedures to maintain an effective control environment. Topic 20905 and other sections of the Commonwealth Accounting Policies and Procedures (CAPP) Manual require each agency to "publish its own policies and procedures documents, approved in writing by agency management." Management should ensure detailed policies and procedures exist for all critical business areas. In addition, management should continue to develop a process to review and approve all policies and procedures either annually or as needed and maintain documentation of the process.

- Professional and Occupational Regulation does not have up to date information security policies and procedures. The Information Security Officer has drafted information security policies and procedures; however, management has not formally approved and annually reviewed the drafts. Professional and Occupational Regulation should establish and approve information security policies and procedures to align with the requirements in the Security Standard. Professional and Occupational Regulation should also develop a process to annually review its information security policies and procedures and document the review to maintain a revision history.

- Professional and Occupational Regulation does not provide role-based security awareness training for users with privileged roles and access, such as System Owners, Data Owners, and System Administrators in accordance with the Security Standard and the Commonwealth's Security Awareness Training Standard, SEC527. Professional and Occupational Regulation should administer role-based training to users with designated security roles.

- Professional and Occupational Regulation did not obtain the System and Organization Controls (SOC) report for a provider that processes sensitive information. As such, Professional and Occupational Regulation did not document an evaluation of the SOC report and the complementary user entity controls described within the report. CAPP Manual Topic 10305 requires agencies to have an adequate level of interaction with third-party providers to give agencies an understanding of the providers' internal control environments and any complementary controls the agency would need to implement. Agencies must also maintain oversight of the provider to gain assurance over outsourced operations. Professional and Occupational Regulation should develop policies and procedures for the review of SOC reports and obtain and comprehensively evaluate SOC reports timely.

- Professional and Occupational Regulation did not ensure individuals in positions of trust properly filed statement of economic interests (SOEI) forms. We identified multiple individuals in a position of trust who either did not submit the SOEI form or did not submit the SOEI form timely. Per § 2.2-3114 of the Code of Virginia, persons occupying positions of trust within state government or non-salaried citizen members of policy and supervisory boards shall file a disclosure statement with the Commonwealth's Ethics Advisory Council, as a condition to assuming office or employment, and thereafter shall file such a statement

annually on or before February 1. Professional and Occupational Regulation should ensure that all individuals identified as employees within positions of trust file the appropriate disclosures upon hire or promotion, and subsequently at each annual filing.

We discussed these matters with management on August 21, 2024. 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 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,

Staci A. Henshaw
Auditor of Public Accounts

JDE/vks

COMMONWEALTH of VIRGINIA
Department of Professional and Occupational Regulation

Glenn A. Youngkin
Governor

G. Bryan Slater
Secretary of Labor

Brian P. Wolford
Director

September 18, 2024

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

Re: Agency Response to Internal Control Questionnaire Review Results

Dear Ms. Henshaw:

Thank you for the opportunity to review and comment on the findings identified in the "Results Memorandum." During the period of the Internal Control Questionnaire review, we were pleased to work with your courteous and professional staff.

In response to the reported observations and recommended improvements, please note the agency's actions to date:

Professional and Occupational Regulation continues to not have adequate controls over audit logging and monitoring as required by the Commonwealth's Information Security Standard, SEC 530 (Security Standard). Specifically, Professional and Occupational Regulation does not enable logs for three out of four sensitive systems. Professional and Occupational Regulation should ensure its sensitive systems record audit logs according to the Security Standard and should develop and implement a process to review and retain sensitive system audit logs at least every 30 days.

Professional and Occupational Regulation does not have up to date information security policies and procedures. The Information Security Officer has drafted information security policies and procedures; however, management has not formally approved and annually reviewed the drafts. Professional and Occupational Regulation should establish and approve information security policies and procedures to align with the requirements in the Security Standard. Professional and Occupational Regulation should also develop a process to annually review its information security policies and procedures and document the review to maintain a revision history.

Professional and Occupational Regulation does not provide role-based security awareness training for users with privileged roles and access, such as System Owners, Data Owners, and System Administrators in accordance with the Security Standard and the Commonwealth's Security Awareness Training Standard, SEC 527.

Telephone: (804) 367-8500 9960 Mayland Drive, Suite 400, Richmond, VA 23233-1485 https://www.dpor.virginia.gov

Professional and Occupational Regulation should administer role-based training to users with designated security roles.

- *DPOR response: DPOR recently filled its long vacant Information Security Officer (ISO) position. DPOR's ISO is actively developing or updating security protocols and enforcement of critical security policies. Additional policy comments included in the next section.*

Department of Professional and Occupational Regulation (Professional and Occupational Regulation) has formal, documented policies and procedures over many of its significant business processes. However, during our review, we identified several critical business areas where Professional and Occupational Regulation did not develop a process to review and approve all policies and procedures either annually or as needed to maintain an effective control environment. Topic 20905 and other sections of the Commonwealth Accounting Policies and Procedures (CAPP) Manual requires each agency to "publish its own policies and procedures documents, approved in writing by agency management." Management should ensure detailed policies and procedures exist for all critical business areas. In addition, management should continue to develop a process to review and approve all policies and procedures either annually or as needed and maintain documentation of the process.

- *DPOR response: As part of Agency's business and technological transformation journey, DPOR started its Policy refresh project in May of 2024 to review a total of 57 existing policies. These policies represent DPOR's critical business and functional areas such as Licensing, Enforcement, Information Technology, Administration, Finance, Information Security, Human Resources and other pertinent sections. The policies were divided into a three-phase project for review and refresh to serve current and future agency needs. The three phases were to review 1) Policies created before 2014, 2) Policies created between 2014-2019 and 3) 2020-Current policies. So far, agency has successfully completed Phase 1 & 2 of the project with third and final phase expected to complete by October 2024 with all the policies approved by the Agency Director.*

Professional and Occupational Regulation did not obtain the SOC report for a provider that processes sensitive information. As such, Professional and Occupational Regulation did not document an evaluation of the SOC report and the complimentary user entity controls described within the report. CAPP Manual Topic 10305 requires agencies to have an adequate level of interaction with third-party providers to give agencies an understanding of the providers' internal control environments and any complementary controls the agency would need to implement. Agencies must also maintain oversight over the provider to gain assurance over outsourced operations. Professional and Occupational Regulation should develop policies and procedures over review of SOC reports and obtain and comprehensively evaluate SOC reports timely.

- *DPOR Response: DPOR will review and implement sufficient internal controls regarding review of SOC reports.*

Professional and Occupational Regulation did not properly ensure individuals in positions of trust properly filed statement of economic interests (SOEI) forms. We identified multiple individuals in a position of trust who either did not submit the SOEI form or did not submit the SOEI form timely. Per § 2.2-3114 of the Code of Virginia, persons occupying positions of trust within state government or non-salaried citizen members of policy and supervisory boards shall file a disclosure statement with the Commonwealth's Ethics Advisory Council, as a condition to assuming office or employment, and thereafter shall file such

a statement annually on or before February 1. Professional and Occupational Regulation should ensure that all individuals identified as employees within positions of trust file the appropriate disclosures upon hire or promotion, and subsequently at each annual filing.

- *DPOR response: DPOR's SOEI procedures were put into effect in January 2024. Late or unsubmitted SOEI Reponses as identified during the audit all occurred during an employee transition phase where both the HR and Finance Director positions were vacant or newly filled. DPOR will ensure all SOEI forms are submitted per Sec 2.2-3114 of the COV in the future.*

We appreciate your thorough review and identification of ways to strengthen our effective internal control environment.

Kind regards,

Digitally signed by Brian Wolford
Reason: I am the author of this document
Date: 2024.09.18 11:51:52 -04'00'

Brian P. Wolford
Director

Cc: The Honorable G. Bryan Slater, Secretary of Labor
Jeb Wilkinson, Special Assistant to the DPOR Director
Karen Garland, Human Resources Director
Candi Pearson, Acting Financial Services Director
Alexina Borkey, Information Management