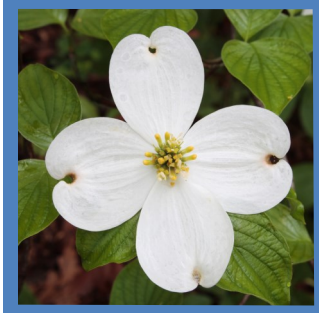

# LIBRARY OF VIRGINIA

# INTERNAL CONTROL QUESTIONNAIRE REVIEW RESULTS AS OF JULY 2019

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

# - TABLE OF CONTENTS -

Commonwealth of Virginia

*Auditor of Public Accounts*

Martha S. Mavredes, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

October 28, 2019

Sandra Treadway, Librarian of Virginia
Library of Virginia
800 East Broad Street
Richmond, VA 23219

## INTERNAL CONTROL QUESTIONNAIRE REVIEW RESULTS

We have reviewed the Internal Control Questionnaire, completed on July 1, 2019, for the **Library of Virginia** (Library). 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 Library 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 Library. 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**

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. 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 Library'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, grants management, contract procurement, and information technology and 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:

- The Library has not developed and documented certain policies and procedures that govern the minimum control requirements for its systems according to the requirements in the Commonwealth's Information Security Standard, SEC 501 (Security Standard). The Library

has a project in place to complete a policy and procedure for each control area in the Security Standard by December 2020. Management should complete the formalized procedures by the target date to ensure compliance with the Security Standard, section 1.4.

- The Library's information technology risk management and contingency planning process and documentation is incomplete and does not include certain attributes needed to effectively evaluate and implement necessary information security controls, including the following items:

    - The information documented in the risk management and contingency planning documents does not align. The Library plans to hire a contractor to review and update the risk management and contingency planning documents to ensure that they correlate. The Library plans to complete the project by September 2020. Management should complete a review and update of its risk management and contingency planning documents by the target date to ensure the documents are consistent and in accordance with the Security Standard, section 3.2.

    - The Library has not completed a risk assessment of each sensitive system within the last three years. The Library completed an enterprise risk assessment in August 2017. However, due to staffing limitations, the Library has not conducted a risk assessment of each sensitive system, as required by the Security Standard, section 6.2. The Library plans to hire a vendor to complete a risk assessment of each sensitive system by August 2020. Management should complete a risk assessment of each sensitive system every three years.

    - The Library does not have a completed Information Technology Disaster Recovery Plan (IT DRP). The Library plans to develop an IT DRP during the risk management and contingency planning update project. Management should develop an IT DRP that documents information technology disaster components for each system necessary to recover business functions or dependent business functions in accordance with Security Standard, sections CP-1-COV-1 and CP-2-COV-2.

- The Library does not conduct a comprehensive Information Technology (IT) security audit on each sensitive system at least once every three years that assesses whether IT security controls implemented to mitigate risks are adequate and effective. The Security Standard requires IT security audits for sensitive systems in accordance with the Commonwealth's IT Security Audit Standard, SEC 502 (IT Audit Standard). The IT Audit Standard, section 1.4, requires that IT systems containing sensitive data, or systems with an assessed sensitivity of high on any of the criteria of confidentiality, integrity, or availability, shall receive an IT security audit at least once every three years. Additionally, the IT Audit Standard, section 2.2,

requires that the IT Security Auditor shall use criteria that, at a minimum, assesses the effectiveness of the system controls and measures compliance with the applicable requirements of the Security Standard. Management should evaluate potential options and develop a formal process for conducting IT audits over each sensitive system at least once every three years that tests the effectiveness of the IT security controls and compliance with Security Standard requirements.

We discussed these matters with management on October 1, 2019. 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

LIBRARY OF VIRGINIA

Sandra Gioia Treadway
*Librarian of Virginia*

November 20, 2019

Martha S. Mavredes, CPA
Auditor of Public Accounts
PO Box 1295
Richmond, VA 23218

Dear Ms. Mavredes:

The Library of Virginia acknowledges receipt of the Internal Control Questionnaire (ICQ) results letter on October 28, 2019. Please accept this letter as the Library of Virginia's response.

As a result of the 2015-2016 audit the Library of Virginia was able to hire one staff member dedicated to the Information Security Program. At the time of hire, the focus of the program was to mitigate outstanding audit report items. This included but was not limited to developing/conducting Risk Assessments, Business Impact Analyses, Disaster Recovery documentation, and improving system access controls.

After that point, the Information Security Program has been focusing on improving staff training, awareness of internal controls, and procedures that pertain to security. Due to major changes in the systems and applications, documentation is currently in refinement to ensure it is up to date with the most current version of the Commonwealth of Virginia Information Security Standard (SEC501). Due to these recent changes in system environment, all risk management, continuity of operations, and disaster recovery related documentation will be re-assessed and up to date by the timeframes provided within the results letter.

Due to budgetary constraints, the Information Security Program has not been able to facilitate comprehensive security audits of each system labeled sensitive. Before embarking on these audits, the Library is in process of assessing each system's proper sensitivity level. Once completed, we will follow with audits per the IT Audit Standard (SEC502).

Please let me know if you have any questions or need any additional information.

Sincerely,

Sandra G. Treadway

Sandra Gioia Treadway

800 East Broad Street
Richmond, Virginia 23219

www.lva.virginia.gov

804.692.3500 *phone*
804.692.3976 *tyy*