



VIRGINIA MUSEUM OF NATURAL HISTORY

INTERNAL CONTROL QUESTIONNAIRE REVIEW RESULTS AS OF SEPTEMBER 2025

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



- TABLE OF CONTENTS -

	<u>Pages</u>
REVIEW LETTER	1-5
AGENCY RESPONSE	6



Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

November 21, 2025

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

Joe Keiper
Executive Director, Virginia Museum of Natural History

INTERNAL CONTROL QUESTIONNAIRE REVIEW RESULTS

We have reviewed the Internal Control Questionnaire for the **Virginia Museum of Natural History** (Museum). We completed the review on September 9, 2025. 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 the Museum 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 the Museum. 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 all prior review findings. The agency has taken adequate corrective action with respect to review findings reported in the prior review 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 for the Museum. Further, we evaluated the Museum'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; expenses; capital assets; 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 (First Issued in 2019)** – The Museum does not have sufficient documented information technology (IT) security governance in accordance with the Commonwealth's Information Security Standard, SEC 530 (Security Standard). The Museum did not have policies and procedures that incorporate the applicable security controls outlined in the Security Standard. In addition, the Museum did not have proper separation of duties within information system security responsibilities. The Museum did not have a designated Chief Information Officer or Chief Information Security Officer. The Security Standard requires proper segregation of duties between these roles and responsibilities. Management should update its policies and procedures and incorporate, at a minimum, the applicable security controls outlined in the Security Standard and delegate the role assignments in a manner that provides adequate separation of duties, provides adequate protection against the possibility of fraud, and does not lead to a conflict of interests. Additionally, the Museum should ensure that those individuals with these roles and responsibilities have the appropriate level of training and knowledge base to perform their duties.

- **Repeat (First Issued in 2019)** – The Museum has made progress to improve risk management and contingency planning. The Museum continues to work with Virginia Information Technologies Agency (VITA) to determine the proper classification for its systems. However, the Museum could not provide a complete documented IT risk assessment for all systems. In addition, the Museum could not provide a Continuity of Operations Plan and a Disaster Recovery Plan. The Museum should continue working with VITA to properly classify systems and meet the requirements of the Security Standard.
- The Museum did not identify its sensitive systems; and therefore, did not conduct an information technology security audit over each of its sensitive systems at least once every three years. The Museum obtained an agreement to perform this service with VITA. The Commonwealth's IT Security Audit Standard, SEC502, requires that IT systems containing sensitive data, or with a sensitivity rating of high on any criteria of confidentiality, integrity, or availability, shall receive an IT security audit at least once every three years. Management should ensure VITA conducts IT audits over each of the sensitive systems at least once every three years and review the results to help ensure the protection of sensitive and mission-critical data.
- The Museum relies on VITA to perform many of its information systems functions based on two memoranda of understanding (MOU) established between the two agencies. However, these MOUs are outdated. The Museum should continue working with VITA to obtain and maintain up-to-date MOUs and ensure there are clearly defined responsibilities for both parties in all areas covered by the MOUs.
- The Museum did not obtain the System and Organization Controls (SOC) report for providers who process sensitive information. As such, the Museum did not perform an evaluation of the SOC report and the complimentary user entity controls described within the report. Commonwealth Accounting Policies and Procedures (CAPP) Manual Topic 10305 and the Security Standard require the Museum to have an adequate level of interaction with third-party providers to give the Museum an understanding of the providers' internal control environments and any complementary controls the Museum would need to implement. The Museum must also maintain oversight of the provider to gain assurance over outsourced operations. The Museum should develop policies and procedures over review of SOC reports for third-party providers and obtain and comprehensively evaluate SOC reports timely.
- The Museum does not have documented security administration processes to ensure that management approves all network and applications access. In addition, the Museum did not review users that have system access at least annually to ensure that access is reasonable as required by the Security Standard. The Museum should annually review and document all users' access to ensure network and applications access is reasonable and properly approved.

- The Museum did not log activity and monitor its systems within 30 days as required by the Security Standard. The Security Standard requires agencies to review information security records at least every 30 days for indications of inappropriate or unusual activity. The Museum should ensure timely completion of audit logging and monitoring reviews.
- The Museum is not properly tracking its ongoing construction costs. CAPP Manual Topic 30205 states that the agency should accumulate ongoing construction costs in the Commonwealth's capital asset system as construction in progress (CIP) using a CIP schedule and track all costs using a CIP asset category. The Museum does not maintain a CIP schedule and does not track assets by asset category. Additionally, the Museum's policies and procedures do not include specific guidance for CIP tracking. The Museum should track assets in accordance with CAPP Manual requirements to properly account for construction costs.
- The Museum's physical inventory listing does not include all capital assets recorded in the Commonwealth's capital asset system. Management noted it removed some older assets due to renovations and others are in storage. However, CAPP Manual Topic 30515 requires agencies to reconcile the physical inventory listing to the Commonwealth's capital asset system and ensure the listing reflects all active assets. The Museum should reconcile its physical inventory records with the Commonwealth's capital asset system to ensure proper stewardship of assets and compliance with CAPP requirements.
- The Museum did not perform a sufficient analysis of potential aggregated assets in accordance with Governmental Accounting Standards Board Implementation Guide 2021-1 Question 5.1, Department of Accounts guidance email, and CAPP Manual Topics Section 30000. The Museum should obtain an understanding of the relevant guidance, develop a process for evaluating aggregated assets, perform an analysis to determine aggregated assets, and record the capitalizable aggregated assets in the Commonwealth's capital asset accounting system.
- The Museum did not record capital asset additions accurately or timely. For one capital asset reviewed, the Museum entered the asset in the Commonwealth's capital asset system nine months after the acquisition date, resulting in the Museum recording the asset in the incorrect fiscal year. Additionally, the Museum recorded the capital asset with a salvage value of approximately 50 percent of the acquisition cost. This salvage value significantly undervalues the capital asset and does not comply with CAPP Manual Topic 30210 guidance. Management should record all capital assets timely in accordance with CAPP Manual Topics 30105 and 30205. The Museum should also revise its valuation methodology to align with CAPP Manual guidance and ensure consistent and accurate recording in the Commonwealth's capital asset system.

- The Museum has formal, documented policies and procedures over many of its significant business processes. However, during our review, we identified critical business areas where the Museum should develop or improve policies and procedures to maintain an effective control environment. Topic 20905 and other sections of the 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 retain documentation of the process.

We discussed these matters with management on September 9, 2025. 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 the Governor and General Assembly, management, and the citizens of the Commonwealth of Virginia and is a public record.

Sincerely,

Staci A. Henshaw
AUDITOR OF PUBLIC ACCOUNTS

JDE/vks

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

Dear Ms. Henshaw,

Thank you for the opportunity to comment on the Auditor of Public Accounts Results letter
Dated November 21, 2025.

The Virginia Museum of Natural History has begun addressing areas of concerns outlined
in the results letter and plans on having all concerns address within the next two years.

Kind Regard,



Dr. Joe Kieper

Executive Director

15 Dec. 2025

15 Dec. 2025