



## DEPARTMENT OF AVIATION

# INTERNAL CONTROL QUESTIONNAIRE REVIEW RESULTS AS OF JUNE 2021

Auditor of Public Accounts  
Staci A. Henshaw, CPA

[www.apa.virginia.gov](http://www.apa.virginia.gov)

(804) 225-3350



## - TABLE OF CONTENTS -

	<u>Pages</u>
REVIEW LETTER	1-4
AGENCY RESPONSE	5-8



Staci A. Henshaw, CPA  
Auditor of Public Accounts

# Commonwealth of Virginia

*Auditor of Public Accounts*

P.O. Box 1295  
Richmond, Virginia 23218

January 24, 2022

Greg Campbell  
Department of Aviation  
5702 Gulfstream Road  
Richmond VA 23250

## INTERNAL CONTROL QUESTIONNAIRE REVIEW RESULTS

We have reviewed the Internal Control Questionnaire for the **Department of Aviation** (Aviation). We completed the majority of the review on June 15, 2021; however, the information system security portion of the review was not completed until November 16, 2021. 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 Aviation 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 Aviation. 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 year 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 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 Aviation'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, expenses, contract and grants management, and information technology (IT) 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:

- **Repeat** - Aviation does not meet all of the minimum requirements of Accounts' ARMICS standards. Management should document and perform current ARMICS processes in compliance with the Commonwealth Accounting Policies and Procedures (CAPP) Manual Topic 10305 and all minimum requirements are addressed.
- **Repeat** - Aviation is not reporting a loan receivable for bridge loans extended to select grantees with federally eligible projects. Aviation has not collaborated with Accounts and made any progress towards reporting these loans due to turnover in the position responsible for these efforts. Management should collaborate with Accounts to determine how to properly report these loans for inclusion in the Commonwealth's Annual Comprehensive Financial Report. Management should also strengthen policies and procedures to ensure they include reporting of bridge loans receivables to Accounts.

- **Repeat** - The Aviation IT Risk Management (RM) and Contingency Planning (CP) process and documentation is incomplete and does not include certain attributes needed to effectively evaluate and implement necessary information security controls in accordance with the Commonwealth's Information Security Standard, SEC 501 (Security Standard). We communicated the control weaknesses to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under § 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms. Aviation should update their RM and CP documentation and ensure the documents are consistent. Aviation should then implement the security controls discussed in the communication marked FOIAE in accordance with the Security Standard.
- **Repeat** - Aviation does not manage security controls over one sensitive system in accordance with best practices. Aviation is making progress to address a weakness communicated in our prior year report; however, the corrective action remains in progress. We identified and communicated the specific control weakness to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms. In general, this weakness related to hardening processes, including reviews and updates. Management should evaluate the best way to mitigate the specific risk communicated in the FOIAE document and comply with best practices.
- Aviation has not implemented a process for contract administrators to periodically document their monitoring of contractor performance. Contract administrators should compile a tracking report on all payments made against a contract and retain documented evidence such as performance reports, journals, etc., when actively monitoring contractor performance. Additionally, Aviation should ensure that contract administrators reconcile such evidence to the approved invoices.
- Aviation does not have complete policies and procedures for all critical business processes. Topic 20905 and other sections of the CAPP Manual state that each agency needs to "publish its own policies and procedures documents, approved in writing by agency management." Management should document and periodically review policies and procedures for all critical business processes in order to maintain an effective control environment and ensure continuity of operations if key personnel are unavailable.
- Aviation does not have a formal process to manage its third-party Software as a Service (SaaS) provider that falls under the purview of the Virginia Information Technologies Agency's (VITA) Enterprise Cloud Oversight Service (ECOS). Therefore, Aviation has not gained annual assurance that the SaaS provider that hosts one sensitive and mission essential system has effective operating controls to protect critical and confidential data. Specifically, Aviation has not signed a formal Memorandum of Understanding (MOU) with VITA's ECOS to obtain the required services to assist the agency with gaining assurance that its SaaS provider implements the minimum-security requirements required by the Commonwealth's Hosted

Environment Information Security Standard, SEC 525 (Hosted Environment Security Standard). Additionally, Aviation does not have a policy or procedure that assigns roles and responsibilities to ensure the correct employees, such as contract administrators or system owners, work with VITA's ECOS to receive and review communications from the SaaS provider. Aviation should develop formal policies and procedures to monitor and maintain oversight of its third-party SaaS provider to ensure they comply with the Hosted Environment Security Standard. Aviation should establish oversight services with VITA's ECOS via a formal MOU, then ensure that VITA's ECOS is meeting all requirements in the MOU.

We discussed these matters with management on September 28, 2021, and January 5, 2022. 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,

Staci A. Henshaw  
Auditor of Public Accounts

JDE\clj



# COMMONWEALTH OF VIRGINIA

Greg Campbell  
Director

**Department of Aviation**  
5702 Gulfstream Road  
Richmond, Virginia 23250-2422

V/TDD – (804) 236-3624  
FAX – (804) 236-3635

March 10, 2022

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

Dear Ms. Henshaw:

This letter serves as the Department of Aviation's comments on the Internal Control Questionnaire Review Results, dated January 24, 2022. We have reviewed the document and offer the following actions and responses to the findings and recommendations.

We appreciate your department's assistance in understanding and addressing areas of need in the Department of Aviation.

## **Review Results**

- **Repeat** - Aviation does not meet all of the minimum requirements of Accounts' ARMICS standards. Management should ensure that the current ARMICS processes are documented and performed in compliance with the Commonwealth Accounting Policies and Procedures Manual Topic 10305 and all minimum requirements are addressed.

*The agency completed the ARMICS review and submission in September 2021. In October, we implemented quarterly testing of fiscal processes to allow us to identify areas requiring improvement prior to fiscal year end. We believe this will help in addressing noted concerns. While we have been performing the requirements for ARMICS, we concur that procedures need to be documented in writing.*

- **Repeat** - Aviation is not reporting a loan receivable for bridge loans extended to select grantees with federally eligible projects. Aviation has not collaborated with Accounts and made any progress towards reporting these loans due to turnover in a position responsible for these efforts. Management should collaborate with Accounts to determine how to properly report these loans for inclusion in the Commonwealth's Annual Comprehensive Financial Report. Management should also strengthen policies and procedures over this area and ensure they include reporting of bridge loans receivables.

*Due to changes in personnel, the agency could find no evidence of this original finding being addressed, resulting in a repeat finding. Since the notification of this repeat finding, the agency has held meetings*



*with the Department of Accounts (DOA) to determine if, when or how bridge loans are to be reported as receivables. The DOA representative is working internally to identify how the agency should proceed.*

- **Repeat** - The Aviation IT Risk Management (RM) and Contingency Planning (CP) process and documentation is incomplete and does not include certain attributes needed to effectively evaluate and implement necessary information security controls in accordance with the Commonwealth's Information Security Standard, SEC 501 (Security Standard). We communicated the control weaknesses to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under § 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms. Aviation should update their RM and CP documentation and ensure the documents are consistent. Aviation should then implement the security controls discussed in the communication marked FOIAE in accordance with the Security Standard.

*The agency concurs with this finding and is working to complete and maintain the IT Risk Management and Contingency Planning processes.*

- **Repeat** - Aviation does not manage security controls over one sensitive system in accordance with best practices. Aviation is making progress to address a weakness communicated in our prior year report; however, the corrective action remains in progress. We identified and communicated the specific control weaknesses to management in a separate document marked FOIAE under § 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms. In general, these weaknesses related to hardening processes, including reviews and updates. Management should evaluate the best way to mitigate the specific risks communicated in the FOIAE document and comply with best practices.

*The IT security audit performed in 2018 for this system identified 16 weaknesses. The agency worked with the vendor and successfully resolved or mitigated those 16 findings as of December 2020. Another security audit was performed in December 2021-February 2022 and resulted in four new findings. Two of these findings involved hardening processes and the remaining two have been mitigated.*

- Aviation has not implemented a process for contract administrators to periodically document their monitoring of contractor performance. Contract administrators should compile a tracking report on all payments made against a contract and retain documented evidence such as performance reports, journals, etc., when actively monitoring contractor performance. Additionally, Aviation should ensure that contract administrators reconcile such evidence to the approved invoices.

*In accordance with the Agency Procurement and Surplus Property Manual, each Contract Administrator is provided a memorandum outlining their responsibilities. These responsibilities include the verification of goods received and invoice review and approval. The memorandum also includes instructions on how to proceed if the vendor services are not meeting expectations and reporting these concerns to the procurement manager for further action. Each contract administrator reviews and signs the memorandum indicating understanding of their responsibilities. The electronic receiving process is one of the tools used to ensure that the invoice, purchase order, and receiver are*



*in agreement. Quantities in excess of the purchase order cannot be received in eVA. While the tracking of payments by the contract administrator is not an APSPM or CAPP requirement, the agency is researching the option of implementing this tool as another level of reconciliation.*

- Aviation does not have complete policies and procedures for all critical business processes. Topic 20905 and other sections of the Commonwealth Accounting Policies and Procedures Manual state that each agency needs to “publish its own policies and procedures documents, approved in writing by agency management.” Management should document and periodically review policies and procedures for all critical business processes in order to maintain an effective control environment and ensure continuity of operations if key personnel are unavailable.

*The agency has created policies and procedures for the majority of critical business processes, the exception being ARMICS documented processes and procedures. We also reviewed current reconciliation procedures to identify areas needing improvement. In October, the agency implemented a thorough reconciliation process for all critical business functions that is conducted on a monthly basis. Existing policies and procedures created by the agency designate the primary and secondary positions responsible for designated tasks.*

- Aviation does not have a formal process to manage its third-party Software as a Service (SaaS) provider that falls under the purview of the Virginia Information Technologies Agency’s (VITA) Enterprise Cloud Oversight Service (ECOS). Therefore, Aviation has not gained annual assurance that the SaaS provider that hosts one sensitive and mission essential system has effective operating controls to protect critical and confidential data. Specifically, Aviation has not signed a formal Memorandum of Understanding (MOU) with VITA’s ECOS to obtain the required services to assist the agency with gaining assurance that its SaaS provider implements the minimum security requirements required by the Commonwealth’s Hosted Environment Information Security Standard, SEC 525 (Hosted Environment Security Standard). Additionally, Aviation does not have a policy or procedure that assigns roles and responsibilities to ensure the correct employees, such as contract administrators or system owners, work with VITA’s ECOS to receive and review communications from the SaaS provider. Aviation should develop formal policies and procedures to monitor and maintain oversight of its third-party SaaS provider to ensure they comply with the Hosted Environment Security Standard. Aviation should establish oversight services with VITA’s ECOS via a formal MOU, then ensure that VITA’s ECOS is meeting all requirements in the MOU.

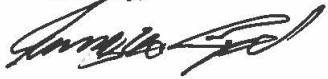
*The agency concurs that additional work on policies and procedures are needed with regard to third-party Software as a Service (SaaS) applications. The application in question was in operation prior to the implementation of the Enterprise Cloud Oversight Service (ECOS). While the agency attempted to navigate the process, there were issues that required guidance from VITA, which created additional delays. Since APA’s review, the application in question is now under the purview of the ECOS program.*

Auditor of Public Accounts  
March 10, 2022  
Page 4

We thank you for the time, attention, and detail you have put into this report. We welcome the opportunity to identify and correct the areas of weakness in an effort to strengthen our agency and its programs. While we have made progress in many areas, we understand there is work still to do.

Please let us know if additional information is needed.

Sincerely,

A handwritten signature in black ink, appearing to read "Gregory W. Campbell", written in a cursive style.

Gregory W. Campbell  
Director