VIRGINIA

DEPARTMENT OF FIRE PROGRAMS

REPORT ON AUDIT

FOR THE PERIOD

JULY 1, 2017 THROUGH MARCH 31, 2019

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

AUDIT SUMMARY

Our audit of the Virginia Department of Fire Programs (Fire Programs) internal controls and compliance over financial reporting, procurement and contract management, payroll and human resources, information technology and security, vehicle management, and grants management for the period July 1, 2017, through March 31, 2019, found:

- matters involving internal control and its operation necessary to bring to management's attention; and

- instances of noncompliance with applicable laws and regulations or other matters that are required to be reported.

In our prior-year special report we identified that Fire Programs did not have a sufficiently strong internal control environment. While there have been some improvements in this area since the last review, there are still several factors with the current control environment that are contributing to the audit findings noted in the section entitled "Audit Scope Overview and Findings by Audit Area." The lack of a strong control environment and internal control structure is a major factor leading to the internal control concerns noted throughout this report and creates a greater opportunity for fraud or errors to occur. Management should take the necessary steps to strengthen the control environment by creating a culture and attitude that supports the importance of maintaining internal controls. Chart 1 below shows the number of findings by audit area.

Findings by Audit Area

Chart 1

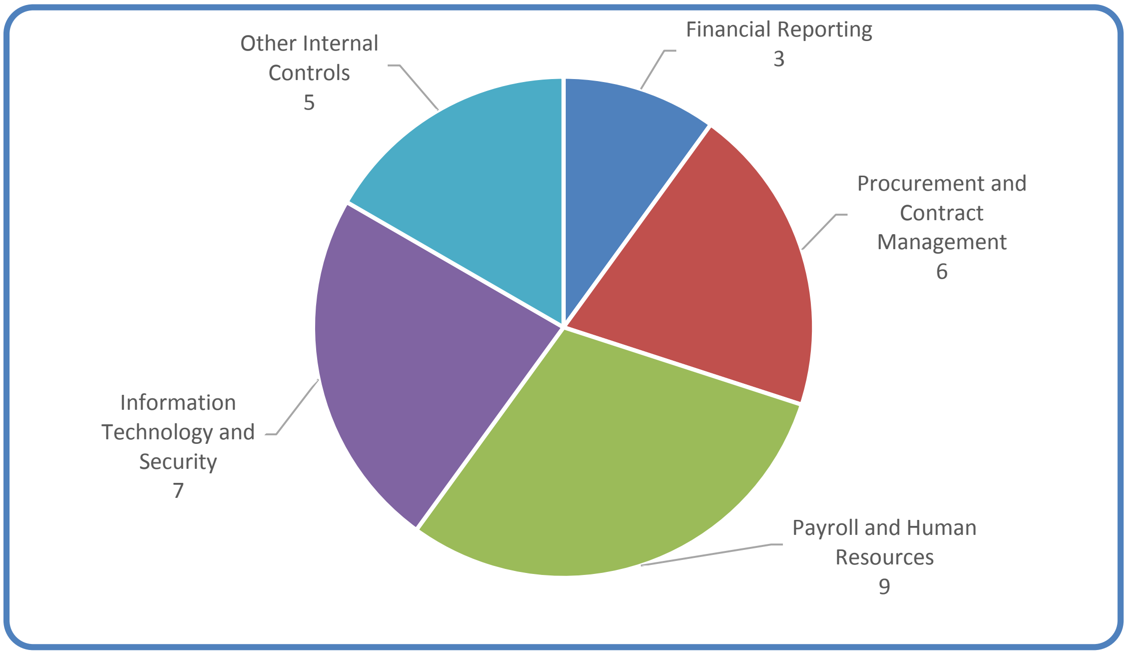


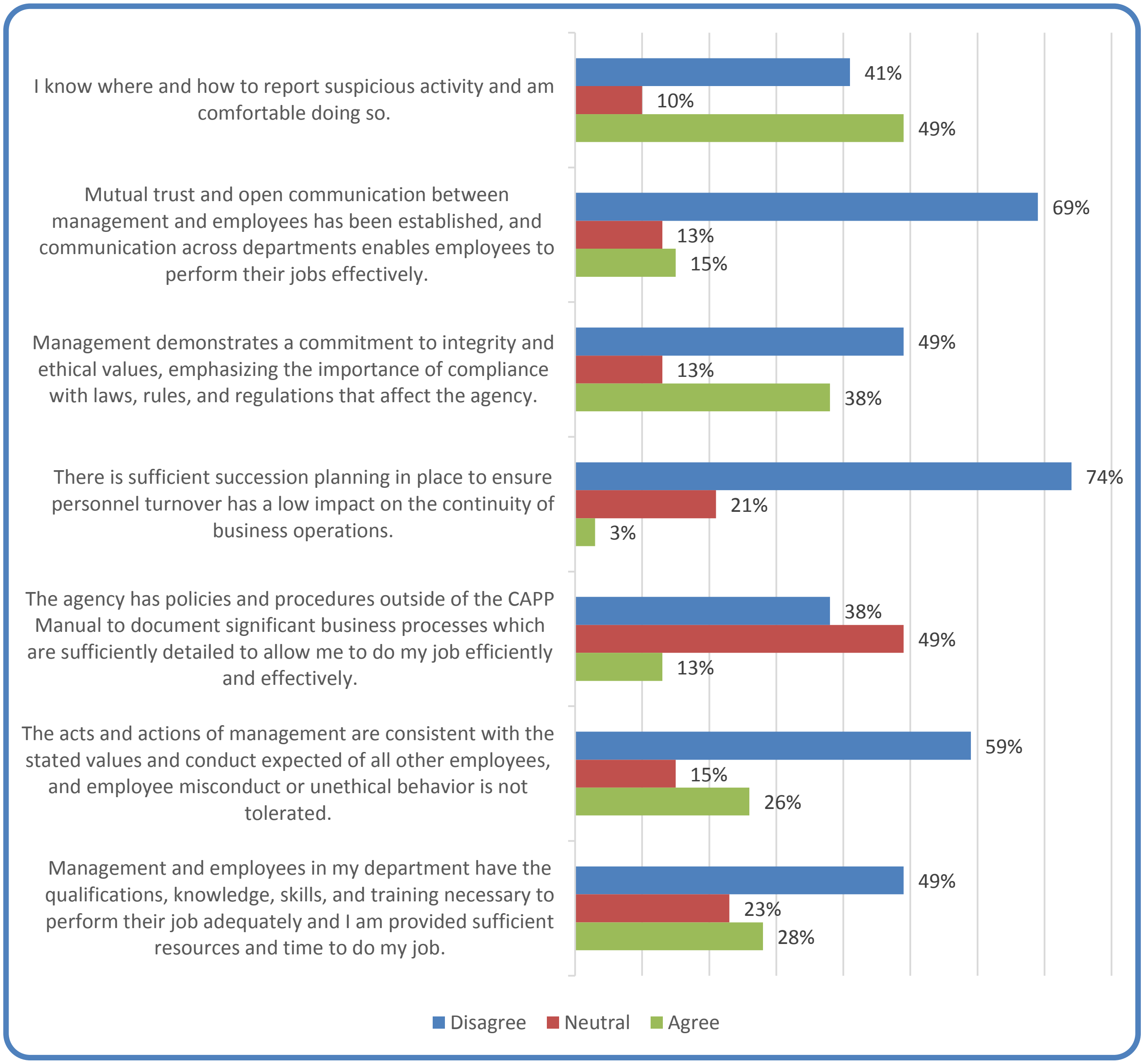
TABLE OF CONTENTS

COMMENT TO MANAGEMENT

In our prior-year special report we identified that the Virginia Department of Fire Programs (Fire Programs) did not have a sufficiently strong internal control environment. While there have been some improvements in this area since the last review, there are still several factors with the current control environment that are contributing to the audit findings noted in the section entitled "Audit Scope Overview and Findings by Audit Area." We conducted in person interviews with several employees and we also sent a survey to all employees outside of executive management to further evaluate the control environment. A total of 39 employees responded to the survey which represents over half of all full-time employees. A selection of questions and responses from the survey is shown below in Chart 2.

Employee Survey Results

Chart 2



The control environment is defined as the set of policies, standards, processes, and structures that provide the basis for maintaining an effective system of internal controls within an organization. The control environment is the foundation for all other components of internal control. Management is responsible for establishing and setting expectations for the control environment, including promoting a positive culture and attitude regarding the importance of maintaining controls. This is often referred to as “the tone at the top.” In recent years, Fire Programs’ control environment has significantly weakened. Several factors that have caused the decline in the control environment include, but are not limited to:

- *Low employee morale*: During this audit we again noted low morale among many employees. We also noted that many employees continued to feel they did not have an avenue to have their concerns addressed, while others felt they would be retaliated against if they spoke out about their concerns. This is further evidenced by the survey results shown in Chart 2 above which displays that 41 percent of respondents do not know how nor feel comfortable reporting suspicious activity. In addition, 69 percent of respondents did not feel there is mutual trust and communication between management and employees. Finally, 49 percent stated that management does not demonstrate a commitment to integrity and ethical values.

- *A lack of succession planning and backups*: As shown in Chart 2 above, in our survey of employees, 74 percent of respondents disagreed that there is sufficient succession planning in place.

- *Significant employee turnover in recent years:* 32 percent of current employees started with the agency within the last three years.

- *A lack of formalized policies and procedures for all critical business processes*: We noted many critical areas where no policies and procedures exist, including reconciliations for all accounting and payroll processes, systems access, conflict of interest filing and training, information technology, and executive leave. In addition, in areas where policies and procedures do exist, many have not been updated for several years and; therefore, are outdated. This includes travel, small purchase charge cards, electronic procurement, and accounting functions. The lack of policies and procedures leads to inconsistencies in the way transactions are processed and duties are performed throughout the agency. In addition, as shown in Chart 2 above, 38 percent of the respondents to our employee survey do not believe the agency has sufficient policies and procedures.

- *Management’s reactive approach to addressing issues with internal controls:* Management does not assess or monitor the overall internal control environment, but rather deals with each problem individually as they occur. This is evidenced by the repeated years of not complying with Department of Accounts Agency Risk Management and Internal Control Standards as detailed further below.

The lack of a strong control environment and internal control structure is a major factor leading to the internal control concerns noted throughout this report. In addition, the current environment with the significant lack of internal controls creates a greater opportunity for fraud or errors to occur. Management should take the necessary steps to strengthen the control environment by creating a culture and attitude that supports the importance of maintaining internal controls. This would include having established policies and procedures for all critical business processes, ensuring that everyone, including top management, consistently follow the policies and procedures, and having open lines of communication for employees to be able to report concerns.

AUDIT SCOPE OVERVIEW AND FINDINGS BY AUDIT AREA

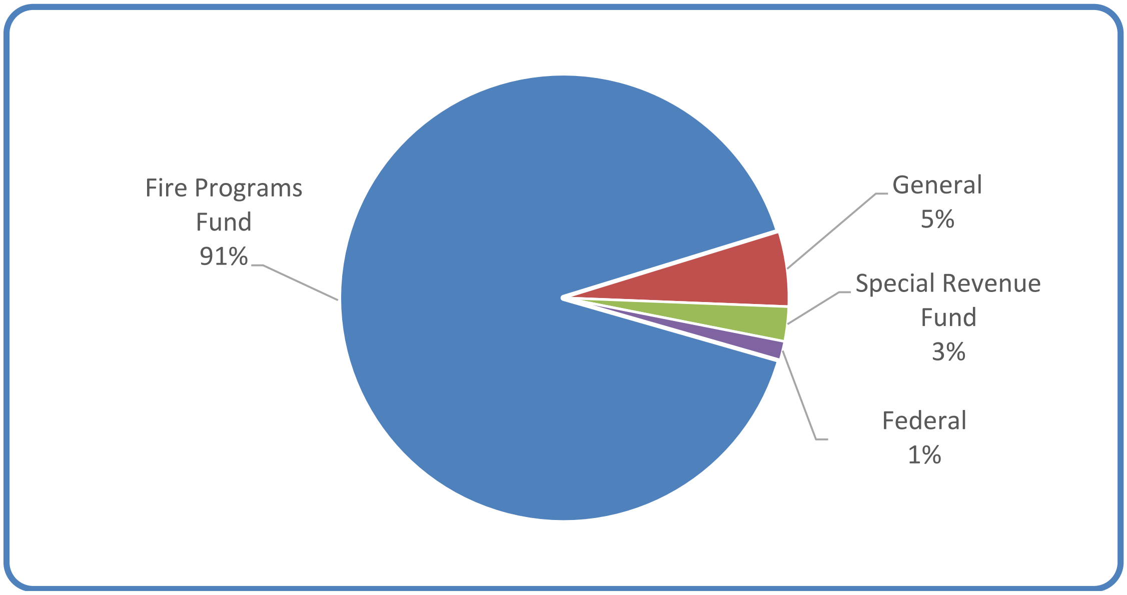
Agency Overview

Fire Programs provides funding, professional development, operational support and technical assistance, data collection and research, and fire prevention inspections for both professional and volunteer fire departments throughout the Commonwealth. The agency is organized into three branches: Administration, Training, and State Fire Marshal's Office. Seven division offices, located throughout the state, support the agency mission. The Administration Division manages the areas within our audit scope, including financial reporting, procurement and contract management, payroll and human resources, information technology and security, vehicles, and legislative actions and compliance with Code of Virginia requirements. The Chief Administrative Officer and Administration Manager have the primary responsibility for oversight of these areas with input from the Deputy Executive Director.

Fire Programs receives the majority (91 percent) of their funding (approximately $38 million) through an annual transfer from the State Corporation Commission that is deposited into the Fire Programs Fund. The transfer is comprised of an annual assessment of all insurance companies that write insurance covering fire, other property and casualty, marine, homeowners, and farm owners. Chart 3 breaks out the annual revenues by fund.

Fiscal Year 2018 Annual Revenues by Fund

Chart 3

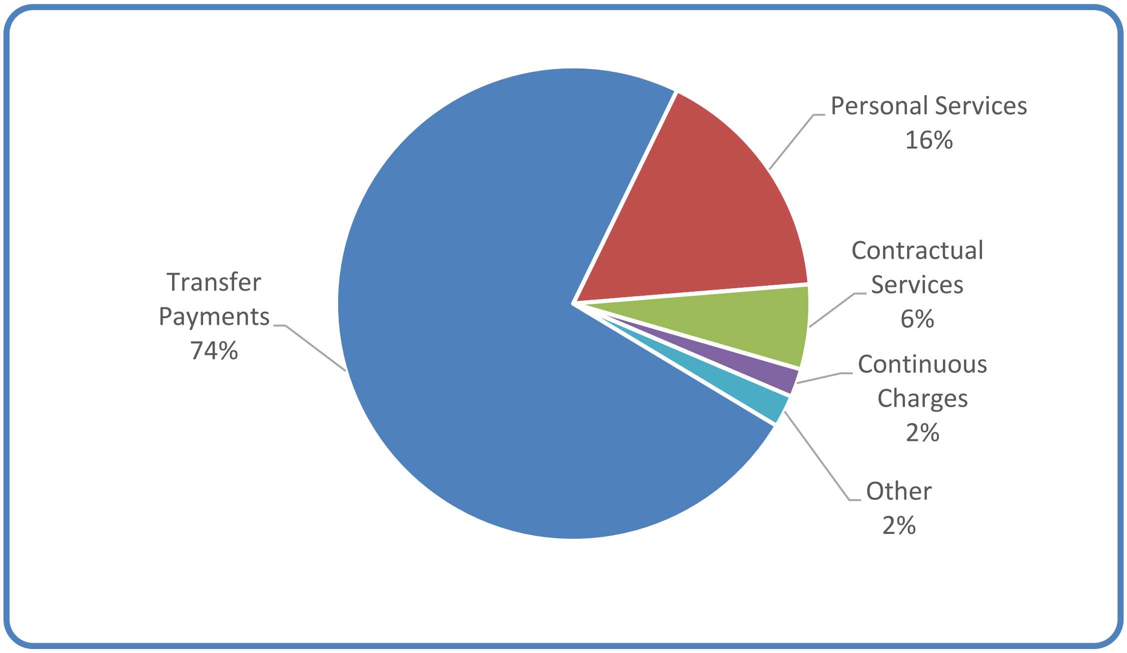


Source: Commonwealth's Accounting and Financial Reporting System

The majority of the Fire Programs Fund is mandated to be spent on aid to localities, including grants for dry hydrants and burn buildings. Approximately 74 percent of the agency expenses are transfer payments to localities. Personal services is the next largest expense, comprising 16 percent of annual expenses. Chart 4 provides an overview of expenses by type.

Fiscal Year 2018 Expenses by Type

Chart 4



Source: Commonwealth's Accounting and Financial Reporting System

Financial Reporting Findings

Comply with Department of Accounts Standards for ARMICS Testing

Type: Internal Control
Included in ICQ Report: Yes
Prior Title: Agency Risk Management and Internal Control Standards (ARMICS)

Fire Programs does not meet the minimum requirements outlined in the Department of Accounts' (Accounts) Agency Risk Management and Internal Controls (ARMICS) standards. The agency certified to Accounts in September of 2018, that there were no weaknesses in internal controls; however, they were unable to provide sufficient documentation to ensure that relevant internal controls were tested. Management indicated that the Administration Manager interviewed personnel responsible for each fiscal area; however, there is no documentation of the date interviews occurred or when tests of controls performed. In addition, Fire Programs does not have procedures for performance and documentation of testing prior to certifying ARMICS.

Pursuant to the Code of Virginia, §§ 2.2-800 and 2.2-803, agencies are required to implement internal control programs. Specifically, Accounts' ARMICS standards indicate that all agencies must comply with the standards as they relate to all government activities that involve the state's assets, accounting, and financial reporting. In addition, the Commonwealth Accounting Policies and Procedures (CAPP) Manual Topic 10305 requires agencies to perform testing to identify strengths, weaknesses, and risks over the recording of financial transactions. Furthermore, Topic 10305 specifically describes the requirement that agencies must document, evaluate, and test agency-level controls across the five components of internal control. Topic 10305 also states that agencies may not certify to Accounts unless they have performed the requirements of ARMICS.

Agency-level controls permeate the agency and have a significant impact on how it achieves its objectives relating to the recording of financial transactions, compliance with financial reporting requirements, compliance with laws and regulations, and stewardship over Commonwealth assets. The agency must demonstrate that they have adequately assessed and tested the five components of internal control. Not completing the required tasks to ensure proper controls are in place puts Fire Programs at risk of improper recording of financial transactions.

Fire Programs has no formal procedures for completion of tasks required to certify ARMICS. Employees assigned to perform the testing do not have the background and training to ensure internal controls are in place.

Fire Programs should establish written procedures for annual ARMICS processes to include testing of controls and the proper documentation that should be retained. Management should ensure that all employees performing tasks related to ARMICS are informed of the requirements and should ensure that all requirements are met prior to certifying ARMICS compliance to Accounts.

Formalize Financial Policies and Procedures

Type: Internal Control
Included in ICQ report: Yes

Fire Programs does not have formalized policies and procedures for their financial processes. This includes processes with respect to cash receipts, cash disbursements, accounts payable, and accounts receivable. The agency, in general, relies on the CAPP Manual and the ARMICS guidelines as their agency policies. Management provided copies of these manuals and guidelines stamped “draft” for all requests for policies and procedures.

The CAPP Manual Topic 20905, and other sections, requires each agency to develop its own internal policies and procedures that are approved in writing by management. The agency’s policies and procedures should be updated regularly to reflect current operations. In addition, best practices indicate that an agency should document, review, and update policies and procedures frequently to ensure the documentation is clear, concise, and adequately addresses operational risks identified. A lack of clearly documented and updated policies and procedures increases the risk of inconsistent application of internal control processes and subsequent inaccurate financial reporting.

Management indicates that due to limited resources they have not been able to devote sufficient resources to comprehensively document policies and procedures for all financial processes. Without formalized policies, agency personnel cannot perform their fiscal duties accurately and consistently. In addition, if errors are made there is nothing to maintain accountability.

Fire Programs should strive to create a control environment that ensures compliance with Commonwealth accounting policies. This includes ensuring that procedures for all fiscal processes including cash receipts, disbursements, receivables, and payables are established, documented, maintained, and communicated to all personnel. Well-documented procedures provide guidance for current operations and will allow a smooth transition in the event of personnel turnover.

Formalize Policies and Procedures for Monthly Reconciliations
Type: Internal Control
Included in ICQ report: No

Fire Programs does not have documented policies and procedures for monthly reconciliations for the Commonwealth's accounting and financial reporting system (financial system). The CAPP Manual Topic 20905 requires that agencies have detailed written procedures for meeting all financial system reconciliation requirements.

Management indicates that due to limited resources they have not been able to devote sufficient resources to comprehensively document policies and procedures for this process. Without formalized policies, there is an increased risk that agency personnel will not process transactions accurately and consistently, and increases the risk that errors will not be detected. Further, management may be unable to hold employees responsible for properly completing reconciliations.

Fire Programs should require that accounting personnel document detailed reconciliation policies and procedures. Once drafted, management should review procedures for thoroughness and accuracy, formally adopt the procedures, and provide them to affected personnel.

Procurement and Contract Management Overview and Findings

The Procurement Department is comprised of two employees, a manager and purchasing analyst. Both are certified as Virginia Contracting Officers (VCO) and; therefore, are cognizant of the requirements for procurement of goods and service for the Commonwealth.

Approximately six percent of Fire Programs' annual expenses are for contractual services. While not a significant amount, proper contract procurement and administration for all contracts and purchase card transactions is necessary for compliance with the Virginia Public Procurement Act and the Department of General Services guidelines.

Procurement and Contract Management Findings

Comply with Contract Administration Requirements
Type: Internal Control
Included in ICQ report: No

Fire Programs does not assign contract administrators for agency contracts. For six of seven (86 percent) of contracts reviewed, there was no documentation that an administrator was assigned. The Agency Procurement and Surplus Property Manual (APSPM), Chapter 10, requires that each contract be assigned an administrator in writing with clearly outlined responsibilities.

Fire Programs management does not want employees overly inundated with forms and requirements and; therefore, instructed the Purchasing Manager not to send out the contract administrator assignment. Not having an assigned contract administrator with designated responsibilities increases the risk that contract billing and payment errors will occur. In addition, Fire Programs cannot be assured that specific contract performance occurs and could pay for services not within the contract scope. Fire Programs should comply with all APSPM requirements which should include ensuring that contract administrators are assigned in writing for all contracts.

Ensure Proper Administration of the Commonwealth's Purchasing System
Type: Internal Control
Included in ICQ report: No

Fire Programs does not properly manage access to the Commonwealth's purchasing system as follows:

- Fire Programs did not appoint a backup security officer for all of fiscal year 2018 and through the second quarter of fiscal year 2019.
- Fire Programs' Security Officer did not remove system access timely for 12 of 23 (52 percent) terminated employees with purchasing system access. This access was removed between 11 and 442 days late.
- The Security Officer did not perform the required quarterly access reviews during fiscal year 2018 and the first quarter of fiscal year 2019.

The Commonwealth's purchasing system security standards require:

- appointment of a backup security officer;
- terminations be reported immediately to the applicable security officer so action can be taken to deactivate access as needed; and
- access reviews to be performed and documented each quarter in part to ensure inactive employees do not have access and system access reflects end-user job duties.

Inappropriate or unnecessary access to the agency's purchasing system reduces management's ability, in the normal course of performing their assigned functions, to prevent, or detect errors on a timely basis. In addition, there is an increased risk of fraudulent purchases by terminated employees with purchasing system access. Timely submission of the request to delete access for terminated employees is imperative to safeguard the assets of the Commonwealth. Not appointing a backup security officer; untimely deactivation of system access for terminated employees; and absence of quarterly reviews is due to a lack of oversight by the prior Security Officer.

Fire Programs management should ensure that the current Security Officer obtains adequate training and understanding of the Commonwealth's purchasing system to effectively perform the duties required. In addition, management should ensure a backup security officer is appointed immediately to perform the required duties in the event the Security Officer is not available.

Formalize Policies and Procedures for the Commonwealth's Purchasing System
Type: Internal Control
Included in ICQ report: No

Fire Programs does not have formalized policies and procedures for the Commonwealth's purchasing system. The agency relies on an outdated version of the Commonwealth Purchasing System Security Manual (Purchasing System Manual) for their purchasing processes.

The Purchasing System Manual and the APSPM, Section 14.3, require each agency to develop its own internal policies and procedures to include re-delegation of purchasing authority, requisition approval process, incorporation of terms and conditions, interface with finance and accounting, recordkeeping, encumbrance of funds, and receiving. Additionally, guidelines should be included for conducting compliance audits/reviews of purchase transactions made by or on behalf of agency employees. Management indicates that due to limited resources they have not been able to devote sufficient resources to comprehensively document policies and procedures for this process.

Without formalized policies, there is an increased risk that agency personnel will not process transactions accurately and consistently. In addition, if errors are made there is nothing to maintain accountability.

Fire programs should strive to create a control environment that ensures compliance with the Purchasing System Manual and the APSPM. This includes well-documented procedures providing guidance for current operations and all future purchases.

Perform Proper Administration of Contracts
Type: Internal Control
Included in ICQ report: No

Fire Programs does not perform proper contract administration for a large contract to implement a new system. Since the initial procurement process in fiscal year 2017, the agency has not received any contract deliverables. In addition, the original contract administrator left the agency in October 2018, and no replacement administrator was assigned. The contract has gone through numerous updates and changes in scope with no documentation, review, price reasonableness calculations or evidence of approval by the contracting officer.

The APSPM, Section 10.2, requires that each contract be assigned an administrator in writing with clearly outlined responsibilities. Additionally, APSPM 10.12 requires that contract files contain documentation of all contract changes, negotiations, or other contract specific events.

Fire Programs management is not fully cognizant of the requirements of contract administration, as they are not procurement professionals. They have not finalized the policies and procedures provided by the Purchasing Manager that clearly speak to proper administration and adherence to the APSPM.

Not having an assigned contract administrator with designated responsibilities increases the risk that contract billing and payment errors will occur. In addition, not maintaining documentation of contract changes or other contract events could lead to Fire Services not receiving the proper services or making improper payments to the contractor.

Fire Programs should comply with APSPM requirements on assignment of contract administrators and documentation and retention of contract files. This should include finalizing and approving policies and procedures over the contract administration process and ensuring the procedures are put into practice.

Retain Documentation of SPCC Transaction Limit Increases

Type: Internal Control
Included in ICQ report: No

Fire Programs did not retain documentation of Small Purchase Charge Card (SPCC) temporary limit increases, for five of ten (50 percent) of the cardholders who exceeded their monthly transaction limit.

The CAPP Manual Topic 20355 allows the program administrator (administrator) to approve temporary increases for up to two weeks; however, the administrator must maintain proper documentation to justify the reason for the change. The instances of no documentation occurred prior to the current SPPC administrator being employed. The current administrator consistently maintains documentation of both temporary and permanent increases; however, there are no formalized policies and procedures for SPCC administration to ensure that that the practices of the current administrator will continue if there is turnover in this position. Without formalized policies, there is an increased risk that limit increases will not be allowable or necessary. This also increases the risk of improper card usage.

Fire Programs should develop and maintain policies and procedures specific to SPCC program administration and strive to create a control environment that ensures compliance with the CAPP Manual. This includes well-documented procedures providing guidance for granting and documenting temporary and permanent increases for both individual and monthly transaction limits.

Ensure Timely Preparation of Small Purchase Charge Card Reconciliation

Type: Internal Control
Included in ICQ report: No

Fire Programs did not provide a signed and dated SPCC reconciliation for four of four (100 percent) reconciliations tested. It appears that supervisors reviewed the transactions; however, without a date on the reconciliation, it is impossible to determine whether the reconciliations were performed timely or not.

Per Topic 20355 of the CAPP Manual, a full SPCC reconciliation is required to be prepared prior to receipt of the following month’s statement. The supervisor is required to sign and date the reconciled statement. If a full reconciliation is not completed, it increases the risk that payment will be made for an unauthorized expense. Fire Programs has not provided their staff with adequate policies and procedures governing the SPCC reconciliation process.

Fire Programs should develop a detailed policy for completing SPCC reconciliations, and distribute it to the appropriate staff. Fire Programs should consider developing a cover sheet to be completed with the monthly reconciliation that requires the reviewer to sign and date it once the process is complete.

Payroll and Human Resources Overview and Findings

As noted above, payroll and benefit expenses are Fire Programs' second largest annual expense. Fire Programs contracts with the Payroll Service Bureau and the Department of Human Resource Management to perform the majority of duties related to payroll and personnel. However, Fire Programs still has certain tasks for which they are responsible to ensure employees are classified properly and paid accurately and timely, and that employee benefits are properly administered.

Payroll and Human Resources Findings

Properly Maintain Wage Employee Records

Type: Internal Control
Included in ICQ report: No

Fire Programs personnel are not properly retaining wage employee records. Personnel files for two of twenty-five (8 percent) employees selected could not be located. CAPP Manual Topic 21005, Records Retention and Disposition, establishes the minimum retention periods for most agency fiscal records, including payroll records. Proper file maintenance and record retention is necessary to ensure that employee compensation is in accordance with the contracted rate.

Fire Programs staff misplaced personnel files during office remodeling. The missing personnel files resulted in the inability to verify the employee's affiliation with the agency and the accuracy of contractual payments. In addition, not properly filing and protecting personnel files increases the risk that employee's information is obtained or used inappropriately.

Fire Programs management should evaluate current procedures for retaining wage employee personnel files. Management should implement corrective measures to ensure that they retain all wage personnel files in accordance with the CAPP Manual.

Comply with Procedures for Reconciling Retirement Benefits System Information

Type: Internal Control
Included in ICQ report: No

Fire Programs does not have sufficient controls in place to ensure retirement information for employees is accurate in the Commonwealth's retirement benefits system. Fire Programs did not follow procedures defined as agency's responsibilities by the Payroll Service Bureau in performing the Commonwealth's retirement benefits system reconciliation for three out of three (100 percent) months selected. Fire Programs did not provide sufficient documentation indicating reconciliations between the Commonwealth's human resources system, the Commonwealth's payroll system, and the Commonwealth's retirement benefits system were completed prior to certifying information to the Virginia Retirement System. Additionally, Fire Programs did not confirm retirement contribution snapshots timely for three out of three (100 percent) months selected.

The CAPP Manual Topic 50905 requires agencies to perform a reconciliation between the Commonwealth's human resource system, the Commonwealth's payroll system, and the Commonwealth's retirement benefits system on a monthly basis. CAPP Manual Topic 50410 details the procedures required to perform the reconciliation mentioned above, which includes reconciling creditable compensation and employee personnel data, and reviewing the cancelled records report and automated reconciliation reports. Additionally, Payroll Service Bureau's Scope of Services Manual (PSB Scope of Services Manual) delineates procedural responsibilities for the agency. Procedures and actions, set forth in the PSB Scope of Services Manual, were derived from and are consistent with CAPP Manual policies. Virginia Retirement System Employer Manual requires employers to submit a month's contribution snapshot by the tenth of the following month.

Inaccurate employee data in the retirement system may not be corrected timely when reconciliations are not performed properly. Since the Virginia Retirement System uses the retirement benefits system data to calculate the Commonwealth's pension liabilities, inaccurate data could result in a misstatement in the Commonwealth's financial statements. Untimely certification at the agency level impacts the ability of Accounts to process inter-agency transfers for any differences between the amounts confirmed in the Commonwealth's retirement benefits system and the retirement contributions actually withheld and paid for all agencies across the Commonwealth. Additionally, without sufficient documentation, there is no audit trail to support completion of the reconciliations.

Fire Programs has not educated employees on the procedures set forth in PSB Scope of Services Manual. The employee responsible for reconciling the snapshot prior to confirmation did not provide documentation that would indicate the retirement benefits system reconciliations were completed.

Fire Programs should follow the policies and procedures set by Accounts in the PSB Scope of Services Manual when performing monthly retirement system reconciliations and educate all employees involved in the process on these policies and procedures. Management should ensure that reconciliations are completed timely in order to confirm retirement contribution snapshots by the tenth of the following month and ensure documentation of the reconciliation process is retained.

Comply with Requirements for Executive Leave

Type: Internal Control
Included in ICQ report: Yes

Fire Programs does not comply with the Commonwealth's Executive Leave Policy. Fire Programs does not ensure that they receive and maintain a written leave certification letter for its at-will employees stating that the employee has not exceeded their leave limit during the allotted time period. In addition, Fire Programs was unable to provide documentation of the supervisor's approval of leave taken by the at-will employees during the allotted time period. At-will employees are individuals appointed by the Governor of Virginia, such as Cabinet members or agency heads.

The Commonwealth's Executive Leave Policy states that all at-will employees must obtain, in advance, proper approval from their supervisor before using any leave. Furthermore, it states that all at-will employees must certify, in writing, that they have not exceeded their established leave limit during the allotted time period. In addition, the agency's Human Resources Office must maintain this certification letter and make it available for review by the Auditor of Public Accounts.

Fire Programs has no written policies stating requirements for recordation and approval of leave for "at-will" employees. They maintain a spreadsheet for each "at-will" employee but there are no approvals evident, some spreadsheets are blank, and completed spreadsheets appear to be pre-filled for the year. Without maintaining the leave certification letter and supervisor's approval, Fire Programs cannot provide assurance that at-will employees complied with the provisions set forth within the Commonwealth's Executive Leave Policy.

Management should develop and implement policies and procedures regarding leave for "at-will" employees. These procedures should address maintaining documentation for approval of leave as well as maintaining leave certification letters. Human Resources should ensure that their department and all "at-will" employees are familiar with requirements under the Commonwealth's Executive Leave Policy. Additionally, Human Resources should monitor for compliance with the policy to include ensuring that their "at-will" employees annually submit a written certification letter establishing that they did not exceed their leave limits during the allotted time period.

<u>Improve Controls over Employee Termination Process</u>

Type: Internal Control and Compliance
Included in ICQ report: No

Fire Programs does not properly complete processes for terminated employees. Fire Programs was unable to provide documentation on removal of system access for nine of nine (100 percent) terminated employees tested. Additionally, Fire Programs did not provide documented evidence that the nine terminated employees returned all Commonwealth property.

The CAPP Manual Topic 50320 recommends agencies develop a termination checklist to be completed as part of the termination process. The checklist should provide confirmation of the collection of any access badges, keys, or other property assigned to the employee. In addition, Commonwealth's Information Security Standard, SEC 501 (Security Standard), Section 09.1 AC-2-COV (2.f), states that each agency shall promptly remove access when no longer required.

By not removing access in a timely manner or retaining documentation that Commonwealth property was returned, Fire Programs increases the risk that terminated employees retain physical access to Commonwealth property and unauthorized access to state systems and sensitive information.

While required by the Accounts, Fire Programs does not have termination policies and procedures developed specifically for the agency's operations to govern employee's employment termination process.

Fire Programs should design and implement policies and procedures that clearly communicate responsibilities to ensure timely completion of termination procedures and proper retention of the documentation in the employee records. Fire Programs should retain sufficient documentation as evidence that the termination process was properly completed.

Document Procedures for Completion and Monitoring of Employment Eligibility Forms
Type: Internal Control and Compliance
Included in ICQ report: No

Fire Programs does not properly complete the Employment Eligibility Verification Form (Form I - 9) for newly hired employees.

- One of 17 (6 percent) employees tested did not sign and date Section 1 of the Form I-9.
- Three of 17 (18 percent) employees tested signed Section 1 of the Form I-9 after the first day of employment.
- For one of 17 (6 percent) employees, Fire Programs did not complete Section 2 of the Form I-9 within the required timeframe of three business days of the starting date of employment.

The Immigration Reform and Control Act of 1986 requires that all employees hired after November 6, 1986, have a Form I-9 completed to verify both employment eligibility and identity. Additionally, the U.S. Department of Homeland Security's Guidance for Completing Form I-9 Handbook for Employers issued by the U.S Citizenship and Immigration Services prescribes federal requirements for completing I-9 forms. Not complying with federal requirements could result in civil and/or criminal penalties and debarment from government contracts. Fire Programs does not have documented policies and procedures outlining the proper completion of the Form I-9, nor do they have a process to monitor these forms for accuracy and completeness.

Fire Programs should create policies and procedures to communicate Form I-9 requirements and provide adequate training and resources to personnel responsible for Form I-9 completion to reinforce the expectation of compliance with the applicable federal requirements. In addition, management should perform an adequate review of I-9 forms completed by personnel to ensure accurate completion and compliance with federal statutes and regulations.

Improve Monitoring of Access to the Commonwealth's Attendance and Leave System
Type: Internal Control and Compliance
Included in ICQ report: No

Fire Programs does not properly terminate access to the Commonwealth's attendance and leave system (system). One terminated employee had HR User Access four months after termination. This is a privileged user role that allows the user to:

- Update employee level and position level information;
- Update leave and timesheets for employees;
- Create batches of transactions to send to the state payroll system; and
- Enter agency-wide configurations.

In addition, this employee's leave balances were not removed from the system upon termination. Fire Program's unwritten process is to remove employee leave balances once the employee has elected to take the leave or have it paid out.

The Security Standard, Section AC-2 (h,) requires notifying account managers when accounts are no longer required; information system users are terminated or transferred, or information system usage or need-to-know changes. In addition, Security Standard, Section AC-2-COV (2.f), states that each agency shall promptly remove access when no longer required.

This instance occurred because Fire Programs does not monitor access, nor do they have policies and procedures to govern system access or the termination process. In addition, the separation checklist that is used does not include removing leave balances. Without prompt removal of access upon termination, there is an increased risk of improper manipulation of critical data, including fraudulent time entry or leave reporting. By not removing leave balances, Fire Programs risks duplicating leave payouts.

Fire Programs should clearly define and document their process for granting and removing system access to ensure that access is appropriate and removed when an employee terminates. Fire Programs should also regularly monitor access to ensure the defined process is being followed. In addition, Fire Programs should ensure that the termination procedures include removing leave balances as appropriate.

Improve Access Approval Process for the Commonwealth's Attendance and Leave System

Type: Internal Control and Compliance
Included in ICQ report: No

Fire Programs does not follow the requirements for access approval for the Commonwealth's attendance and leave system. We noted the following issues with access forms:

- One of ten (10 percent) employees tested signed and approved their own access request form.
- The agency Human Resource Director approval was not evident for six of ten (60 percent) employees tested.
- Two of ten (20 percent) employees had access to a privileged user role when their position should only require an inquiry only role.
- For one of ten (10 percent) employees tested, access granted was more critical than what was authorized on the system access request form.

The Security Standard, Section AC-2 (e), requires the agency receive supervisory approval for requests to create information system accounts. Without appropriate access approval, there is an increased risk of improper manipulation of critical data and employee's having access to sensitive data that is not required as part of their position. In addition, the Security Standard, Section AC-6, requires the agency to employ the principle of least privilege, allowing only authorized access for users that is necessary to accomplish assigned tasks. Fire programs does not have documented policies and procedures for granting system access.

Fire Programs should develop policies and procedures for granting access to the attendance and leave system. In addition, management should ensure that all requests for access to the Commonwealth's attendance and leave system are approved by the appropriate individuals.

Formalize Policies and Procedures for the Payroll Certification Process

Type: Internal Control
Included in ICQ report: No

Fire Programs does not have formalized policies and procedures for payroll certification. The current Accountant Supervisor has developed detailed procedures for her personal use; however, these procedures are informal and have not been approved by management. In addition, prior to fiscal year 2019, no documentation of pre or post certification processes was maintained.

The CAPP Manual Topic 50905 requires that key control totals are maintained in order to facilitate the Report 10/33 Reconciliation. The Report 10/33 Reconciliation helps identify potential problems with payroll records such as pre-tax deductions not being properly taxed, manual payment processing that affected taxable fields incorrectly, or improper withholding of certain taxes. Identifying and correcting discrepancies on a monthly basis facilitates essential quarter and year-end certifications. CAPP Manual Topic 50820, Post-Certification Activities, states that the certifier should perform a post-certification audit of the payroll following processing.

Management indicates that due to limited resources they have not been able to devote sufficient resources to comprehensively document policies and procedures for this process. In addition, due to employee turnover the certification documentation was not retained prior to fiscal year 2019. Without formalized policies, there is an increased risk that payroll changes are made after certification and/or transactions are not processed as intended. Not retaining documentation prevents management from determining if processes were performed timely and accurately.

Fire Programs should review procedures currently outlined by the Accountant Supervisor for thoroughness and accuracy, formally adopt the procedures, and ensure all accounting personnel who could have a payroll responsibility are aware of the procedures. In addition, management should ensure that documentation related to the certification process is consistently retained.

Monitor Wage Employee Hours
Type: Internal Control and Compliance
Included in ICQ report: No

Fire Programs does not adequately monitor employee hours to ensure part-time employees are limited to 1,500 hours annually. For the look-back period from May 1, 2017, through April 30, 2018, we found no employees who exceeded the limit; however, in the current lookback period we are aware of at least one employee who exceeded the limit.

For certain Commonwealth employees, Chapter 836 § 4-7.01 g of the 2017 Virginia Acts of Assembly and the Patient Protection and Affordable Care Act requires that employees not work more than 29 hours per week on average over a twelve-month period. In addition, Human Resource Policy 2.20, developed by the Department of Human Resource Management, states that wage employees are limited to working 1,500 hours per agency per year. This policy was developed to ensure that the Commonwealth is complying with the requirements of the Patient Protection and Affordable Care Act, which could bring penalties for noncompliance.

Fire Programs stopped monitoring the process during fiscal year 2018, and does not have written procedures that require responsible supervisors to review wage employee hours to ensure compliance with the 1,500-hour rule. Fire Programs should implement written policies and procedures related to the monitoring of part-time hours. These should include a procedure to require supervisors to review employee hours each pay period.

Information Technology and Security Overview and Findings

Fire Programs' information technology (IT) systems are vital to its mission and include systems that allow incident reporting by fire departments statewide, and systems supporting the financial and administrative operations. The agency IT department consists of three full-time personnel who are charged with maintaining and monitoring all agency systems. These tasks include granting and removing access, planning for disasters and subsequent recovery, and security awareness training for all employees.

Information Technology and Security Findings

Improve IT Governance
Type: Internal Control and Compliance
Included in ICQ report: No

Fire Programs has an insufficient governance structure to manage and maintain their information security program in accordance with the Security Standard. Section 2.4.2 of the Security Standard requires the agency head to ensure an information security program is maintained that is sufficient to protect the agency's IT systems and that is documented and effectively communicated.

Fire Programs has control weaknesses in the following areas, showing that Fire Programs does not maintain appropriate oversight over their information security program and does not meet the requirements in the Security Standard:

- Lack of Information Security Policies and Procedures
- Unsecured Databases
- Inconsistent IT Risk Management and Contingency Process and Documentation
- Lack of Assurance over Third-Party Providers
- Deficient Security Awareness Training Monitoring
- Insufficient Logging and Monitoring Processes

Not having an appropriate governance structure to properly manage Fire Programs IT environment and information security program can result in a data breach or unauthorized access to confidential and mission-critical data leading to data corruption, data loss, or system disruption if accessed by a malicious attacker, either internal or external. A breach could impact funding to the agency for training career and volunteer responders, conducting research, providing operational and technical assistance to communities during emergencies, and conducting fire prevention inspections.

Fire Programs has limited financial resources and, as a result, has limited IT resources to manage and maintain their information technology and security program. In addition, Fire Programs lacked a designated IT Manager/ISO position to provide oversight for the IT department until 2019.

Fire Programs should develop a formal plan to create and implement information security policies and procedures to manage and maintain their sensitive systems and maintain compliance with the Security Standard. Fire Programs should evaluate the most efficient and productive method to bring their IT security program in compliance with the Commonwealth's security standards. Fire Programs should also evaluate their IT resource levels to ensure sufficient resources are available to implement IT governance changes and rectify any control deficiencies. Implementing these recommendations will help ensure the integrity and availability of Fire Programs' mission essential data.

Develop and Implement Information Security Policies and Procedures
Type: Internal Control and Compliance
Included in ICQ report: Yes

Fire Programs does not have information security policies and procedures to support their information security program. The Security Standard requires Fire Programs to prepare, disseminate, and maintain information security policies, standards, guidelines, and procedures as appropriate to facilitate effective implementation of an information security program.

Without documented and formally approved information security policies and procedures, Fire Programs cannot effectively communicate and implement information security requirements to protect and mitigate risks to sensitive data. Additionally, Fire Programs may inconsistently address security needs in its IT environment, increasing the potential of unauthorized access to data and the inability to recover from system outages timely, among other risks.

Fire Programs lacks documented and approved information security policies and procedures due to limited IT resources and, until recently, Fire Programs did not have an executive level position to manage and oversee IT operations. Fire Programs hired an IT Manager, who will also serve as the Information Security Officer (ISO), in February 2019 to manage IT and information security at the agency.

Fire Programs should dedicate the necessary resources to develop and formally approve information security policies and procedures and implement them into their information security program. The policies should align with the requirements in the Security Standard and establish the minimum requirements to implement effective security controls in Fire Program's IT environment. Developing and implementing the policies will help to ensure the confidentiality, integrity, and availability of data and achieve compliance with the Security Standard.

Improve Database Security

Type: Internal Control and Compliance
Included in ICQ report: Yes

Fire Programs does not secure three databases that support systems they rate as 'High' for confidentiality, integrity and/or availability with certain minimum-security controls in accordance with the Security Standard, and industry best practices.

We communicated the control weaknesses to management in a separate document marked Freedom of Information Act Exempt under § 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms. The Security Standard and industry best practices require the implementation of certain controls that reduce unnecessary risk to data confidentiality, integrity, and availability in systems processing or storing sensitive information.

Fire Programs should ensure database configurations, settings, and controls align with its policies and the requirements in the Security Standard and industry best practices, such as the Center for Internet Security Benchmark. Implementing these controls will help maintain the confidentiality, availability, and integrity of the sensitive and mission critical data stored or processed in the database.

Improve IT Risk Management and Contingency Planning Processes

Type: Internal Control and Compliance
Included in ICQ report: Yes

Fire Programs' IT risk management and contingency planning process and documentation is incomplete and does not include certain attributes to effectively evaluate and implement information security controls in accordance with the Security Standard. Fire Programs risk management and contingency planning processes contain the following weaknesses:

- Fire Programs has not performed an annual review and revision of the Business Impact Analysis since 2017. In addition, Fire Programs does not consistently identify mission essential functions and primary business functions. The Security Standard, Section 3, requires annual reviews of the agency Business Impact Analysis to identify mission essential functions, along with the supporting primary business functions, and correlation of information among the risk management and contingency planning documents. Fire Programs should review and revise the Business Impact Analysis annually to ensure they accurately identify the business functions essential to the agency mission and the resources required.

- Fire Programs is not consistently identifying information systems between the risk management and contingency planning documents. Specifically, the Business Impact Analysis lists three systems that are not in the Continuity Plan, and the Continuity Plan lists five systems that are not in the Business Impact Analysis. Additionally, Fire Programs lists the Online Bookstore system in the Business Impact Analysis and Disaster Recovery Plan but retired the system in 2017. The Security Standard, Section 3.2, requires Fire Programs to use the information in the Business Impact Analysis as a primary input to the other risk management and contingency planning documents. Fire Programs should update and revise all of the risk management and contingency planning documents to ensure they are consistent.

- Fire Programs is not properly and consistently rating the sensitivity of mission essential systems within its risk management and contingency planning documents in accordance with the Security Standard, Sections 3.2.5 and 4.2.4. Specifically, the Business Impact Analysis rates four systems as sensitive and one system as non-sensitive that the Sensitive Systems List does include. The Security Standard requires that each IT system required to recover a mission essential function or primary business function shall be considered sensitive relative to availability. Further, the Security Standard requires that organizations classify an IT system as sensitive if any type of the data handled by the IT system has a sensitivity of high on any of the criteria of confidentiality, integrity, or availability. Fire Programs should establish and implement a policy and process to classify sensitive systems and consistently document the rating of sensitive systems throughout all risk management and contingency planning documents.

- Fire Programs does not have complete and current risk assessments for their sensitive systems. Fire Programs provided draft risk assessments for two systems, dated August 2017 and February 2017, respectively. However, Fire Programs did not finalize and approve the two risk assessments. Additionally, Fire Programs did not conduct and document risk assessments for six other systems rated as ‘High’ for confidentiality, integrity, and/or availability in their risk management and contingency planning documents. Section 6 of the Security Standard requires that Fire Programs conduct and document a risk assessment of each IT system classified as sensitive at least once every three years. Fire Programs should conduct and document a risk assessment for each system it classifies as sensitive.

- Fire Programs does not consistently document recovery time objectives for each business function and supporting IT systems within the Business Impact Analysis and Continuity Plan. The Security Standard, Section 3, requires that Fire Programs document the recovery time objectives for each IT system needed to recover a mission essential function or primary business function. Fire Programs should ensure that they correctly identify and consistently document the recovery time objectives for each business function and supporting IT system among the risk management and contingency planning documentation.

- Fire Programs' IT Disaster Recovery Plan does not include recovery requirements for ten systems that the Business Impact Analysis and/or Continuity Plan list as necessary to recover a mission essential function or primary business function. Fire Programs should develop an IT Disaster Recovery Plan that documents IT disaster components for each system necessary to recover business functions or dependent business functions in accordance with the Security Standard, Sections CP-1-COV-1 and CP-2-COV-2.

- Fire Programs does not conduct and document annual disaster recovery tests to verify their ability to restore each sensitive system. Additionally, Fire Programs has not reviewed and revised the IT Disaster Recovery Plan since February 2017. The Security Standard, Section CP-1-COV, requires that Fire Programs review and revise the IT Disaster Recovery Plan following an annual exercise to reflect lessons learned. Fire Programs should review and revise the IT Disaster Recovery Plan and develop a plan to conduct disaster recovery testing.

Without maintaining current and complete risk management and contingency planning documentation, Fire Programs may not properly identify mission essential functions and the IT resources necessary to support them. This increases the risk that Fire Programs may not be able to recover systems timely in the event of an outage or disaster. Additionally, without current and approved risk assessments, Fire Programs may not adequately secure sensitive systems or upgrade against known vulnerabilities that can impact data confidentiality, integrity, and availability.

A lack of policies and procedures that support the information security program led to inconsistencies among the risk management and contingency planning documents. Additionally, until recently, Fire Programs did not have an executive level position to manage and oversee IT and information security at the agency, but hired an IT Manager, that will also serve as the ISO, in February 2019. Further, Fire Programs updated the Continuity Plan in March 2019, but has not updated the Business Impact Analysis and IT Disaster Recovery Plan since 2017, which contributed to the inconsistencies.

Fire Programs should document and implement a process to manage the information technology risk management and contingency management programs. Fire Programs should update their risk management and contingency planning documentation and ensure the documents are consistent to help protect its sensitive systems and data according to the requirements in the Security Standard.

Improve Oversight over Service Providers

Type: Internal Control and Compliance
Included in ICQ report: Yes

Fire Programs does not gain annual assurance that their third-party service provider has a secure IT environment to protect sensitive data. Third-party providers are organizations that perform outsourced business tasks or functions on behalf of the agency. Fire Programs uses a third-party provider that hosts and stores critical and sensitive data related to certificates of testing from cigarette manufacturers.

The Commonwealth's Hosted Environment Information Security Standard, SEC 525 (Hosted Environment Security Standard), Section SA-9-COV 3.1, requires agencies to perform an annual security audit of the environment or review the annual audit report of the environment conducted by an independent, third-party audit firm on an annual basis. By not gaining assurance over third-party service providers' IT environments, Fire Programs cannot validate that the vendors provide effective IT controls to protect its sensitive data.

Fire Programs does not gain assurance over their third-party providers' IT environments because there is no formal process in their information security program for identifying and gaining annual assurance for their third-party service providers. Thus, there is no expectation to provide the appropriate oversight.

Fire Programs should develop a formal process to gain assurance that their third-party providers have secure IT environments to protect sensitive data. One way to do this is by requesting and reviewing System and Organization Controls reports or by review of other independent audit reports as accepted by the Commonwealth's IT Security Audit Standard, SEC 502. After Fire Programs develops a formal process, they should incorporate it into their information security program.

Improve Security Awareness Training

Type: Internal Control and Compliance
Included in ICQ report: Yes

Fire Programs does not have any policy, procedures, or process to ensure all users complete annual security awareness training. Specifically, Fire Programs does not adequately monitor employees' completion of security awareness training to ensure that all active employees complete annual training. Fire Programs had 14 out of 81 employees, approximately 17 percent, who did not complete the training within the past year.

The Security Standard, Section AT-2, requires annual security awareness training for all computer users. Without a process to ensure all users take security awareness training annually, Fire Programs increases the risk that untrained users will be more susceptible to malicious attempts to compromise sensitive data, such as ransomware, phishing, and social engineering.

A lack of policies and procedures contributed to not all users taking security awareness training. Additionally, until recently, Fire Programs did not have an executive level position to manage and oversee IT operations. Fire Programs hired an IT Manager, who will also serve as the ISO, in February 2019 to manage IT and information security at the agency.

Fire Programs should develop and document a formal process that ensures all users receive annual security awareness training, as well as a process to verify compliance. Improving the security awareness training program will help protect Fire Programs from malicious attempts to compromise the confidentiality, integrity, and availability of sensitive data.

Improve Logging and Monitoring

Type: Internal Control and Compliance
Included in ICQ report: Yes

Fire Programs does not have policies and procedures to support their monitoring and logging process. Additionally, Fire Programs does not identify and monitor high risk system events for potential malicious activity.

The Security Standard requires logging certain events, such as actions executed by administrative users, and following a process for monitoring the logs while using appropriate separation of duties. (*Security Standard, Sections: AU-2 Audit Events, AU-9 Protection of Audit Information, & AU-6 Audit Review, Analysis, and Reporting*)

Without logging and monitoring policies and procedures and not monitoring high risk system events, Fire Programs may not identify suspicious activity in a timely manner or adequately protect and maintain the integrity of system logs. Fire Programs has insufficient monitoring controls due to a lack of formal policies and procedures to govern the process. Additionally, Fire Programs has limited IT resources.

Fire Programs should develop policies and procedures for logging and monitoring system events that align with the requirements in the Security Standard. Fire Programs should identify high risk events and have the appropriate personnel monitor system activity for their sensitive systems. Implementing the proper monitoring controls will enable Fire Programs to protect the confidentiality, integrity, and availability of its mission critical and sensitive data.

Other Internal Controls

Executive management is ultimately responsible for overall agency operations, to include establishment of internal controls, ensuring internal controls are functioning effectively, monitoring of legislative actions, and ensuring compliance with all applicable regulations. As in all areas noted previously, the lack of documented policies and procedures hinders management's ability to oversee and administer the agency goals and missions.

Other Internal Control Findings

Ensure Proper Tracking of Laws and Regulations
Type: Internal Control
Included in ICQ report: No

Fire Programs is not properly tracking changes to legislation that could have an effect on the agency. Fire Programs could not provide sufficient documentation to show that they are monitoring laws and regulations to ensure they are in compliance with the most recent changes. The listing, provided by Fire Programs, simply consisted of titles from the Code of Virginia, Appropriation Act, and Virginia Administrative Code. The listing did not address how the changes in legislation would affect the agency or who was responsible for managing the changes. This is not sufficient documentation to ensure that Fire Programs will comply with new legislation.

Fire Programs does not have internally created policies and procedures related to the legislative tracking process. The CAPP Manual Topic 20905 states "As with every topic in this manual, CAPP manual procedures alone never eliminate the need and requirement for each agency to publish its own internal policies and procedures, approved in writing by management. The lack of complete and up-to-date internal policies and procedures, customized to reflect the agency's staffing, organization, and operating procedures, reflects inadequate internal control." A lack of documented policies and procedures for tracking legislation increases the risk that Fire Programs would not track legislation consistently and thoroughly to ensure it is in compliance with all applicable laws and regulations.

Fire Programs should strive to provide all employees with the appropriate policies and procedures that relate to their job responsibilities. This includes ensuring that procedures for legislative tracking processes are established, documented, maintained, and communicated to all necessary personnel. The procedures should include creating a tracking mechanism that will indicate who is responsible, what changes are anticipated to comply, and the necessary timeframe.

Formalize Process to Ensure Compliance with Statement of Economic Interest Filing
Type: Internal Control
Included in ICQ report: No

Fire Programs does not have documented policies or procedures to ensure all employees designated as occupying a position of trust submit their annual filing timely. Pursuant to the Code of Virginia § 2.2-3100, all employees in a position of trust must complete the Statement of Economic Interest (SOEI) filing by February 1 of each year.

Fire Programs is proactive in its determination of who should file, monitors these employees to ensure timely filing, and is rigid in their communication with employees to complete the filing on time. For the February 1, 2019 filing, all but one of the 57 employees designated as in a position of trust filed by the deadline. However, while Fire Programs has an informal process, it does not have formal documented procedures for either determination of who should file or to ensure filings are completed timely. This lack of documented procedures increases the risk that an employee who should file does not and those who are required to file do not do so timely.

Fire Programs should ensure compliance with SOEI requirements by creating, implementing, and maintaining written policies and procedures to meet Code of Virginia requirements for the SOEI filings. These policies should incorporate guidance issued by the Commonwealth's Ethics Council.

Comply with Conflict of Interest Training Requirements
Type: Internal Control and Compliance
Included in ICQ report: No

Fire Programs' SOEI Coordinator (Coordinator) is not ensuring that employees in a position of trust complete the required Conflict of Interest training within two months of employment and every two years, thereafter. In addition, Fire Programs does not maintain records of training attendance as required. Of the 57 employees required to file the SOEI, there is no documentation that any of the required filers completed training within two months of their employment and/or within the prior two years.

The Code of Virginia §§ 2.2-3128 through 2.2-3131 requires that each SOEI filer complete Conflict of Interest Act training within two months of employment and at least once every two years. This training is designed to help filers recognize potential conflicts of interest. As of December 1, 2015, the Ethics Council offers an orientation video on their website, which satisfies this requirement. Filers who register and watch the entire video get credit for taking the training. As required by Code of Virginia § 2.2-3129, each agency must maintain, for a minimum of five years, records of who completed the orientation course. Due to the lack of policies and procedures for the SOEI process in general, the coordinator does not keep records of training taken and is unable to determine who has taken the training, and when they completed the training.

Because Fire Programs does not maintain records of the required training and does not ensure training is completed timely, Fire Programs may be limited in its ability to hold its employees accountable for not knowing how to recognize a conflict of interest and how to resolve it. Additionally, filers could be subject to penalties for inadequate disclosure as outlined at Code of Virginia §§ 2.2-3120 through 2.2-3137. While Fire Programs is proactive in identifying employees required to file and communicating reminders for timely filing, they have not attended to the orientation requirements.

The coordinator should obtain the Conflict of Interest Act training records as required by the Code of Virginia. Fire Programs should use these records to ensure that employees in positions of trust complete the training once within each consecutive period of two calendar years. Additionally, Fire Programs should maintain the attendance records for a minimum of five years.

Improve Internal Controls over Fuel Reconciliation

Type: Internal Control
Included in ICQ report: No

Fire Programs does not have adequate internal controls over Voyager fuel card usage. Fire Programs did not review and maintain supporting documentation for three of four (75 percent) months of fuel reconciliations reviewed.

The OFMS Policies and Procedures Manual requires the Fuel Card Custodian ensure that users of fuel cards turn in receipts of purchases from commercial retail fuel sites. The Fuel Card Custodian is also required to maintain records of all card usage, sign out sheets, receipts, and other applicable documents.

Without proper receipts for fuel purchases, Fire Programs cannot confirm that fuel was purchased for a legitimate business purpose. In addition, since regulations require that only regular fuel be purchased unless unavailable, there is no way to determine the fuel type. Review of a Voyager card statement would only show that a purchase was made, but would not necessarily show that the payment was for fuel or the fuel type.

Fire Programs did not provide policies and procedures to employees for fuel card usage. Additionally, the employee responsible for the fuel reconciliations did not require compliance with the requirement to maintain receipts.

Fire Programs should provide employees with policies and procedures governing fuel purchases using the Voyager card. Fire Programs should also ensure that all gas receipts are reviewed and retained with the fuel reconciliations to ensure that all purchases are business related and comply with all Commonwealth requirements.

Formalize Policies and Procedures for Tracking Aid to Localities

Type: Internal Control
Included in ICQ report: Yes, significant progress made

Fire Programs does not have formal policies and procedures in place for the process of tracking and monitoring aid provided to localities. In our prior audit we noted that monitoring of aid provided to localities was not performed. Fire Programs currently performs a detailed desk review of funds provided to localities, and has developed a process for completing onsite audits of locality expenses. However, documentation of these processes is lacking.

The current process appears to be sufficient; however, the CAPP Manual as well as best practice dictates that significant processes for an agency be included in a formal policy and procedure that is approved by management. The Grants and Budget Manager has developed a detailed review procedure for funds requests and also a process for on-site audits of the most risky localities who do not submit expense documentation; however, this is currently not formalized or approved by management. Not having formalized policies and procedures creates the risk that this function will not continue if there is staff turnover. In addition, having the policies and procedures approved by management ensures that the process is accurate and in line with other agency processes.

Fire Programs should strive to formalize and complete detailed policies and procedures for the monitoring process to include the following procedures:

- Review of annual request from locality with and without documentation
- Completion of locality audit form and website posting
- Determination of payment schedule
- Risk assessment for onsite audits
- Projected timeline/dates for onsite audit completion
- Review process during onsite audit

In addition, Fire Programs should ensure that these policies and procedures are approved by management and regularly reviewed to ensure the process is kept up to date.

Commonwealth of Virginia

Auditor of Public Accounts

Martha S. Mavredes, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

September 18, 2019

The Honorable Ralph S. Northam
Governor of Virginia

The Honorable Thomas K. Norment, Jr.
Chairman, Joint Legislative Audit
and Review Commission

We have audited the **Virginia Department of Fire Programs** (Fire Programs) internal controls and compliance over procurement and contract management, payroll and human resources, information technology and security, vehicle management, and grants management for the period July 1, 2017, through March 31, 2019. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Audit Scope and Objectives

Our audit's primary objectives with regard to procurement and contract management, payroll and human resources, information technology and security, vehicle management, and grants management were to review the adequacy of Fire Programs' internal control and test compliance with applicable laws, regulations, contracts, and grant agreements.

Audit Methodology

Fire Programs' management has responsibility for establishing and maintaining internal control and complying with applicable laws, regulations, contracts, and grant agreements. Internal control is a process designed to provide reasonable, but not absolute, assurance regarding the reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws, regulations, contracts, and grant agreements.

We gained an understanding of the overall internal controls, both automated and manual, as they relate to the audit objectives, sufficient to plan the audit. We considered significance and risk in determining the nature and extent of our audit procedures. We performed audit tests to determine whether Fire Program's controls were adequate, had been placed in operation, and were being followed. Our audit also included tests of compliance with provisions of applicable laws, regulations, contracts, and grant agreements as they pertain to our audit objectives.

Our audit procedures included inquiries of appropriate personnel, inspection of documents, records, and contracts, and observation of Fire Program's operations. We performed analytical procedures, including budgetary and trend analyses. We also tested details of transactions to achieve our objectives.

A nonstatistical sampling approach was used. Our samples were designed to support conclusions about our audit objectives. An appropriate sampling methodology was used to ensure the samples selected were representative of the population and provided sufficient, appropriate evidence. We identified specific attributes for testing each of the samples and when appropriate, we projected our results to the population.

Conclusions

We noted certain matters involving internal control and its operation and compliance with applicable laws, regulations, contracts, and grant agreements that require management's attention and corrective action. These matters are described in the section entitled "Audit Scope Overview and Findings by Audit Area."

Exit Conference and Report Distribution

We discussed this report with management on December 9, 2019. Management's response to the findings identified in our audit is included in the section titled "Agency Response." We did not audit management's response and, accordingly, we express no opinion on it.

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.

Martha S. Mavredes
AUDITOR OF PUBLIC ACCOUNTS

JDE/vks

COMMONWEALTH of VIRGINIA

Virginia Department of Fire Programs

Michael T. Reilly
EXECUTIVE DIRECTOR

Brook Pittinger
DEPUTY DIRECTOR

Office of the Executive Director
1005 Technology Park Drive
Glen Allen, VA 23059-4500
Phone: 804/ 371-0220
Fax: 804/ 371-3444

Monday, December 16, 2019

Martha S. Mavredes
Auditor of Public Accounts
James Monroe Building
101 North 14th Street 8th Floor
Richmond, VA 23219

Management's Response to the 2019 APA Audit

The Auditor of Public Accounts (APA) returned to the Virginia Department of Fire Programs (VDFP) in May 2019 to conduct an in-depth audit of the Agency's administrative activities for the period of July 1, 2017 through March 31, 2019.

The APA had previously issued the 2018 VDFP audit report in November 2018. From November 2018 until the APA returned in May 2019, approximately seven months, VDFP successfully addressed many of the fourteen 2018 audit items, with the remaining items being addressed, but not completed before the 2019 audit commenced. VDFP has performed its due diligence in correcting approximately 80 percent of the items noted in the 2018 audit prior to the start of the May 2019 audit. VDFP has been working diligently since the 2018 APA audit was published and the 2018 audit items that have been addressed or worked on by VDFP with great vigilance.

The 2019 APA Audit was an in-depth audit that expanded the scope of audit findings from the 2018 audit report. The initial report contained thirty-six (36) findings, of which VDFP did not concur with all of the findings. Equipped with this more in-depth information, the Agency has developed a strategy to fully address all APA audit items. We are also cognizant of the IT concerns APA has brought to our attention and are working diligently to address the deficiencies identified. Upon providing our feedback to the APA, the APA did adjust several of the findings. The Agency appreciates the APA's cooperation in this revision and recognizes APA's direction in adopting statewide policies to be adopted into our own.

VDFP will continue to review and evaluate our policies and procedures to determine continual process improvement opportunities. The Agency looks forward to our continued relationship with the APA and the opportunities to improve our business processes.

Sincerely,

Michael T. Reilly

Michael T. Reilly

VIRGINIA DEPARTMENT OF FIRE PROGRAMS

As of March 31, 2019

Michael T. Reilly
Executive Director

Brook Pittinger
Chief Deputy Director

Brenda Scaife
Chief Administrative Officer