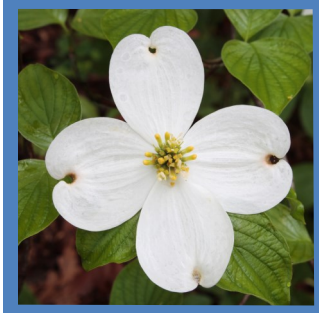


INNOVATION AND ENTREPRENEURSHIP INVESTMENT AUTHORITY AND CENTER FOR INNOVATIVE TECHNOLOGY

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2018

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

AUDIT SUMMARY

Our audit of the Innovation and Entrepreneurship Investment Authority, including its blended component unit, the Center for Innovative Technology, for the year ended June 30, 2018, found:

- the financial statements are presented fairly, in all material respects;
- internal control findings requiring management's attention; however, we do not consider them to be material weaknesses; and
- no instances of noncompliance or other matters required to be reported under Government Auditing Standards.

We have audited the basic financial statements of the Innovation and Entrepreneurship Investment Authority, including its blended component unit, the Center for Innovative Technology, as of and for the year ended June 30, 2018, and issued our report thereon, dated July 31, 2019. Our report is included in the Authority's Annual Report that it anticipates releasing by August 2019.

– TABLE OF CONTENTS –

	Pages
AUDIT SUMMARY	
INTERNAL CONTROL FINDINGS AND RECOMMENDATIONS	1-3
INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS	4-5
AUTHORITY RESPONSE	6-10
AUTHORITY OFFICIALS	11

INTERNAL CONTROL FINDINGS AND RECOMMENDATIONS

Improve Information Security Policies and Procedures
Type: Internal Control
Severity: Significant Deficiency
Repeat: No

The Center for Innovative Technology (CIT) does not align its information security policies and procedures with the Commonwealth's Information Security Standard, SEC 501 (Security Standard) or other industry security standards, such as the National Institute of Standards and Technology's Special Publication 800-53 (NIST Standard). As a result, CIT does not define nor perform a consistent process to obtain assurance that all third-party service providers (provider) that access, store, or process CIT's sensitive data have adequate security controls. Providers are entities that perform tasks or functions on behalf of CIT. CIT relies on several providers for mission-critical business functions, such as hosting its financial system of record, payroll processes, and data center hosting services.

The Security Standard, section 1.1, states organizations that procure IT equipment, systems, and services from providers remain accountable for maintaining compliance with the Security Standard and must enforce these compliance requirements through documented agreements with providers. Additionally, the NIST Standard, section 2.5, states the Federal Information Security Management Act (FISMA) and Office of Management and Budget (OMB) policies require that federal agencies using external providers to process, store, or transmit federal information or operate information systems on behalf of the federal government, assure that such use meets the same security requirements that federal agencies are required to meet.

CIT is not a state or government agency and does not align its information security policies and procedures with an industry security standard, but instead views the industry security standards as a guideline. As a result, CIT's policies and procedures do not include specific requirements to ensure the implementation of certain processes and controls, such as receiving and evaluating independent assurance from its providers. Without CIT having a documented process to gain assurance over providers' internal controls, CIT cannot consistently validate that those providers have effective controls to protect its sensitive data.

CIT should adopt an industry security standard, such as the Security Standard or the NIST Standard, and align its information security policies and procedures accordingly. Additionally, CIT should define and document policies and procedures for maintaining oversight of all providers that access, store, or process sensitive information. Maintaining oversight of all providers will assist CIT in ensuring the confidentiality, integrity, and availability of sensitive and mission-critical data.

Develop and Adhere to Written Policies and Procedures Over System Access
Type: Internal Control
Severity: Significant Deficiency
Repeat: No

CIT does not have written policies and procedures in place for establishing, managing, or terminating employee access to its financial systems. In addition, management does not maintain sufficient documentation to support that they are timely changing or terminating financial systems' access based on changes in employment or job responsibilities. For the two employees who separated during fiscal year 2018 through April 2019, CIT did not retain sufficient physical documentation supporting authorized and timely removal of access to its financial systems.

Best practices for managing system access entail maintaining detailed, written policies and procedures that require management to process access changes timely and to maintain sufficient documentation of adjustments to access. Having adequate policies and procedures is a key component of internal control and ensures consistent processing of access changes for all financial reporting and support systems. Further, system access policies and procedures should support management's function of ensuring access is appropriate for each employee.

Without written policies and procedures over system access, management is increasing the risk of unauthorized and inappropriate access, as well as the risk of compromising the integrity of the organization's financial reporting and support systems. Although management is aware of having and adhering to written policies and procedures regarding system access, management was unable to provide a reason why this component of internal control does not currently exist.

CIT's management should develop and adhere to written policies and procedures surrounding the oversight of system access. These procedures should include controls surrounding the process to grant, modify, or terminate access to all financial reporting and support systems. Management should also ensure the procedures include requirements for retaining documentation that supports the reasonableness and timeliness of changes to system access for CIT employees.

Ensure Proper and Consistent Application of Capital Asset Policies and Procedures
Type: Internal Control
Severity: Significant Deficiency
Repeat: No

CIT's management does not consistently apply estimated useful life ranges for capital assets based on accounting policies and procedures. Within the CIT capital asset listing, there are assets that have useful life estimates that do not align with the ranges established within CIT accounting policies. Further, based on the naming conventions and inadequate project descriptions of some assets listed, we were unable to determine the assets' value, related depreciation, or if it was reasonable for management to capitalize certain assets when applying Government Accounting and Standards Board (GASB) standards.

GASB Codification Section 1400 - Reporting Capital Assets, indicates management should calculate depreciation for capital assets over their estimated useful lives. It further indicates management should measure depreciation expense by allocating the cost of depreciable assets over their estimated useful lives in a systematic and rational manner. The useful life of an asset is management's approximation of a monetary amount in the absence of a precise measurement. The standards also state, if repairs or maintenance do not extend the useful life or capacity of an asset, management should be expensing the cost as incurred. Current accounting policies and procedures sets forth the criteria CIT's management is using for assessing estimated useful life and for capitalizing repairs and maintenance; however, there is currently not enough supporting documentation available to ensure management has been consistently applying these policies over the years. The lack of adequate supporting documentation and inconsistent application can lead to misstatements and unreliable information within the financial statements.

While CIT accounting policies and procedures include useful life ranges and capitalization thresholds to apply to capital assets and its related improvements, management has not consistently applied them when capitalizing assets. Without a clear understanding of the nature of the assets and related projects that management is currently tracking within the entity's asset listing, it is difficult for management to ensure asset values are reasonable and materially correct.

CIT's management should prioritize reviewing and cleaning up its current asset listing to ensure they are not double counting asset values and the related depreciation. Management should also ensure that they are adequately describing assets within the asset listing and that they are able to trace depreciable assets to existing structures. Lastly, management should strengthen existing policies and procedures to ensure consistent application of estimated useful life thresholds.

Commonwealth of Virginia

Auditor of Public Accounts

Martha S. Mavredes, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

July 31, 2019

The Honorable Ralph S. Northam
Governor of Virginia

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

Board of Directors
Innovation and Entrepreneurship Investment Authority and
Center for Innovative Technology

INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS

We have audited, in accordance with the auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in Government Auditing Standards, issued by the Comptroller General of the United States, the financial statements of the **Innovation and Entrepreneurship Investment Authority**, including its blended component unit, the Center for Innovative Technology, as of and for the year ended June 30, 2018, and the related notes to the financial statements, which collectively comprise the Authority's basic financial statements, and have issued our report thereon dated July 31, 2019.

Internal Control Over Financial Reporting

In planning and performing our audit of the financial statements, we considered the Authority's internal control over financial reporting to determine the audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the Authority's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of the Authority's internal control over financial reporting.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Our consideration of internal control over financial reporting was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control over financial reporting that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that were not identified. Given these limitations, during our audit we did not identify any deficiencies in internal control over financial reporting that we consider to be material weaknesses. We did identify certain deficiencies in internal control over financial reporting entitled "Improve Information Security Policies and Procedures," "Develop and Adhere to Written Policies and Procedures Over System Access," and "Ensure Proper and Consistent Application of Capital Asset Policies and Procedures," which are described in the section titled "Internal Control Findings and Recommendations," that we consider to be significant deficiencies.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the Authority's financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts and grant agreements, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit and, accordingly, we do not express such an opinion. The results of our tests disclosed no instances of noncompliance or other matters that are required to be reported under Government Auditing Standards.

The Authority's Response to Findings

We discussed this report with management at an exit conference held on August 8, 2019. The Authority's response to the findings identified in our audit is described in the accompanying section titled "Authority Response." The Authority's response was not subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on it.

Purpose of this Report

The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the entity's internal control or on compliance. This report is an integral part of an audit performed in accordance with Government Audit Standards in considering the entity's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

AUDITOR OF PUBLIC ACCOUNTS

LDJ/clj

CIT
CENTER FOR INNOVATIVE TECHNOLOGY

August 6, 2019

Martha Mavredes, CPA
Auditor of Public Accounts
P.O. Box 1295
Richmond, Virginia 23218

Dear Ms. Mavredes:

We have reviewed the audit findings and recommendations resulting from the fiscal year 2018 audit by the Auditor of Public Accounts (APA). The following contains the APA's findings and management's response to the concerns and issues raised.

Findings of the APA:

Improve Information Security Policies and Procedures

The Center for Innovative Technology (CIT) does not align its information security policies and procedures with the Commonwealth's Information Security Standard, SEC501 (Security Standard) or other industry security standards, such as the National Institute of Standards and Technology's Special Publication 800-53 (NIST Standard). As a result, CIT does not define nor perform a consistent process to obtain assurance that all Third-Party Service Providers (Provider) that access, store, or process CIT's sensitive data have adequate security controls. Providers are entities that perform tasks or functions on behalf of CIT. CIT relies on several Providers for mission-critical business functions, such as hosting its financial system of record, payroll processes, and data center hosting services.

The Security Standard, section 1.1, states organizations that procure IT equipment, systems, and services from Providers remain accountable for maintaining compliance with the Security Standard and must enforce these compliance requirements through documented agreements with Providers. Additionally, the NIST Standard, section 2.5, states the Federal Information Security Management Act (FISMA) and Office of Management and Budget (OMB) policies require that federal agencies using external Providers to process, store, or transmit federal information or operate information systems on behalf of the federal government, assure that such use meets the same security requirements that federal agencies are required to meet.

CIT is not a state or government agency and does not align its information security policies and procedures with an industry security standard, but instead views the industry security standards as a guideline. As a result, CIT's policies and procedures do not include specific requirements to ensure the implementation of certain processes and controls, such as receiving and evaluating independent assurance from its Providers. Without CIT having a documented process to gain assurance over Providers'

internal controls, CIT cannot consistently validate that those Providers have effective controls to protect its sensitive data.

CIT should adopt an industry security standard, such as the Security Standard or the NIST Standard, and align its information security policies and procedures accordingly. Additionally, CIT should define and document policies and procedures for maintaining oversight of all Providers that access, store, or process sensitive information. Maintaining oversight of all Providers will assist CIT in ensuring the confidentiality, integrity, and availability of sensitive and mission-critical data.

CIT Management Response:

CIT aligns its information security policies with, and is compliant to, SEC501 for all covered portions of the CIT IT infrastructure. CIT IT policy states:

"The policy relies on a single governance structure based on the Commonwealth of Virginia (COV) SEC501 security policy and associated elements such as Risk Assessment and Business Impact Analysis for all applications, but is partitioned into those applications in the COV/VITA baseline that are compliant to SEC501, and those provided (as allowed by law) as separate IT services needed for the operation of the Center for Innovative Technology stand-alone 501(c)3 organization, which may not be compliant to SEC501."

The CIT policy also calls out additional Federal standards as applicable, for example in cases where CIT engages in Federal contracts that flow down IT requirements. For non-COV portions of the CIT IT infrastructure CIT has adopted the risk management approach of NIST 800-53 (rev 5 draft), primarily as it relates to third party service providers, which states:

"... the controls in the catalog are independent of the specific process employed to select those controls. Such selection processes can be part of an organization-wide risk management process, a life cycle-based systems engineering process, or a risk management or cybersecurity framework. The control selection criteria can be guided and informed by many factors, for example, stakeholder protection needs and concerns; mission and business needs; standards and best practices; and requirements to comply with laws, Executive Orders, directives, policies, and regulations. The comprehensive nature of the security and privacy controls coupled with a flexible, risk-based control selection process, can help organizations comply with applicable security and privacy requirements and achieve adequate security for their information systems."

In this context, and as a matter of practice, CIT annually receives and evaluates independent assurance of security controls from its third party providers, primarily in the form of SOC Type II reports from each provider. However, we agree with the finding that this process is not currently specified as a requirement in the relevant CIT IT policy. In order to formalize and document this practice CIT will update our IT Policy to better reflect our IT practices. This update will incorporate a new policy section relating to third party IT providers, and will incorporate three elements:

- explicitly call out an annual request, acquisition and review by CIT of the SOC-2 reports from each of the third party providers.

- add a policy requirement for a contractual clause(s) requiring vendors to provide the relevant SOC-2 reports at least annually as part of any new contracts or service renewals.

- CIT will formalize the IT risk assessment policy in accordance with NIST 800-53 (rev 5 draft) control RA-1 which in addition to our other existing Policy actions requires the organization to designate a senior management official to manage the risk assessment policy and procedures. We will update our policy to reflect that the CIT CEO will manage the risk assessment policy and procedures, require that the CIO/ISO report directly to the CEO, and require the ISO or other designee to annually summarize any risk findings from third party providers as presented in the SOC-2 reports or elsewhere, characterize those risks, and present the findings to the CEO for formal acceptance of those risks by the Corporation, or remediation of specific risks as directed.

Develop and Adhere to Written Policies and Procedures Over System Access

CIT does not have written policies and procedures in place for establishing, managing, or terminating employee access to its financial systems. In addition, management does not maintain sufficient documentation to support that they are timely changing or terminating financial systems' access based on changes in employment or job responsibilities. For the two employees who separated during fiscal year 2018 through April 2019, CIT did not retain sufficient physical documentation supporting authorized and timely removal of access to its financial systems.

Best practices for managing system access entail maintaining detailed, written policies and procedures that require management to process access changes timely and to maintain sufficient documentation of adjustments to access. Having adequate policies and procedures is a key component of internal control and ensures consistent processing of access changes for all financial reporting and support systems. Further, system access policies and procedures should support management's function of ensuring access is appropriate for each employee.

Without written policies and procedures over system access, management is increasing the risk of unauthorized and inappropriate access, as well as the risk of compromising the integrity of the organization's financial reporting and support systems. Although management is aware of having and adhering to written policies and procedures regarding system access, management was unable to provide a reason why this component of internal control does not currently exist.

CIT's management should develop and adhere to written policies and procedures surrounding the oversight of system access. These procedures should include controls surrounding the process to grant, modify, or terminate access to all financial reporting and support systems. Management should also ensure the procedures include requirements for retaining documentation that supports the reasonableness and timeliness of changes to system access for CIT employees.

CIT Management Response:

CIT has written policies and procedures for managing (onboarding, modifying, removing) employee access to its financial record keeping system, Microsoft Dynamics SL. Management acknowledges that the current written policies and procedures need to be expanded to include the financial support systems and to include requirements regarding timeliness and maintenance of sufficient documentation. CIT is currently in the process of updating the system access policies and procedures.

Ensure Proper and Consistent Application of Capital Asset Policies and Procedures

CIT's management does not consistently apply estimated useful life ranges for capital assets based on accounting policies and procedures. Within the CIT capital asset listing, there are assets that have useful life estimates that do not align with the ranges established within CIT accounting policies. Further, based on the naming conventions and inadequate project descriptions of some assets listed, we were unable to determine the assets' value, related depreciation or if it was reasonable for management to capitalize certain assets when applying Government Accounting and Standards Board (GASB) standards.

GASB Codification Section 1400 - Reporting Capital Assets, indicates management should calculate depreciation for capital assets over their estimated useful lives. It further indicates management should measure depreciation expense by allocating the cost of depreciable assets over their estimated useful lives in a systematic and rational manner. The useful life of an asset is management's approximation of a monetary amount in the absence of a precise measurement. The standards also state if repairs or maintenance do not extend the useful life or capacity of an asset, management should be expensing the cost as incurred. Current accounting policies and procedures sets forth the criteria CIT's management is using for assessing estimated useful life and for capitalizing repairs and maintenance; however, there is currently not enough supporting documentation available to ensure management has been consistently applying these policies over the years. The lack of adequate supporting documentation and inconsistent application can lead to misstatements and unreliable information within the financial statements.

While CIT accounting policies and procedures include useful life ranges and capitalization thresholds to apply to capital assets and its related improvements, management has not consistently applied them when capitalizing assets. Without a clear understanding of the nature of the assets and related projects that management is currently tracking within the entity's asset listing, it is difficult for management to ensure asset values are reasonable and materially correct.

CIT's management should prioritize reviewing and cleaning up its current asset listing to ensure they are not double counting asset values and the related depreciation. Management should also ensure that they are adequately describing assets within the asset listing and that they are able to trace depreciable assets to existing structures. Lastly, management should strengthen existing policies and procedures to ensure consistent application of estimated useful life thresholds.

CIT Management Response:

Management acknowledges that there are inconsistences in the application of useful life ranges for capital assets based on accounting policies and procedures. In regards to the original building construction capital assets, management believes the reasonable explanation for the varying estimated lives is that the building additions made in years subsequent to the initial construction were depreciated over estimated lives to end at the same time as the initial construction, since the additions did not extend the life of the building. Management is unable to confirm whether the policies and procedures in effect at the time the building was constructed, 25 – 30 years ago, included information regarding estimated lives of building additions. Inconsistences of estimated useful lives for assets acquired more recently are the result of mistakes in applying the policy. The current written policies and procedures are broad in scope and will be updated to provide a more detailed process for determining estimated useful lives of capital assets, as well as the controls for ensuring that the policies are followed.

Management's view is that the capital asset values are reasonable and materially correct. The finding related to naming conventions and project descriptions pertains primarily to building construction costs incurred over 25 years ago. Management's position is that it is appropriate and reasonable to rely on prior management's determinations and financial statement audit reports for the past 30 years stating that the financial statement present fairly, in all material respects, the financial position of the organization. Given that the building has been designated as surplus property by the Commonwealth and is in the process of being sold, management does not intend to perform an in-depth review of the building construction costs at this time. The focus of the asset listing review will be on non-building capital assets that are still being depreciated. The current policies and procedures will be updated and enhanced to ensure that going forward, the method of naming, tracking and depreciating capital assets is clear and provides a sufficient audit trail to the amounts on the financial statements.

Sincerely,

Susan Aitcheson, CPA
Chief Financial Officer

Center for Innovative Technology
2214 Rock Hill Road
Suite 600
Herndon, VA 20170

INNOVATION AND ENTREPRENEURSHIP INVESTMENT AUTHORITY
AND
CENTER FOR INNOVATIVE TECHNOLOGY

As of June 30, 2018

Board of Directors

Michael Steed, Chairman
Walter Mazan, Vice Chairman

Jonathan Aberman
Brian Ball
Ángel Cabrera
Stephen Chapin
Marilyn Crouther
Kristie Helmick Proctor
Angela Kellett
Bernard Mustafa
Atif Qarni
Rob Quartel
Timothy Sands
Teresa A. Sullivan

Officers

Ed Albrigo, CIT President and Chief Executive Officer
Susan Aitcheson, CIT Chief Financial Officer