Assessment and Evaluation of the City of Philadelphia's Information Technology General Controls Fiscal Year 2019

City Controller
Rebecca Rhynhart

August 2020

CITY OF PHILADELPHIA

OFFICE OF THE CONTROLLER
1230 Municipal Services Building
1401 John F. Kennedy Boulevard
Philadelphia, PA 19102-1679
(215) 686-6680 FAX (215) 686-3832

REBECCA RHYNHART
City Controller

CHRISTY BRADY
Deputy City Controller

Tuesday, August 18, 2020

Mark Wheeler
Chief Information Officer
Office of Innovation and Technology
1234 Market Street, Suite 1850
Philadelphia, PA 19107

Dear Mr. Wheeler:

As part of our audit of the city's Comprehensive Annual Financial Report (CAFR) for the fiscal year ended June 30, 2019, the Office of the City Controller engaged the Mercadien Group, who retained BDO USA, LLP, to evaluate the city's Information Technology (IT) general controls over key financial-related applications. Details regarding some of these findings were also included in our annual report on internal control and on compliance and other matters for fiscal year 2019. Please find our full report on the city's IT general controls attached. The report identified four significant deficiencies and several other deficiencies that require your attention.

Notably, the Office of Innovation and Technology (OIT) management has not provided sufficient oversight of the change management function, the process that ensures changes to IT systems are properly approved and tested before the implementation of that change. Specifically, the change management policy provided by OIT did not establish clear procedures for reviewing, testing and documenting changes to the city's IT systems. A lack of oversight in the change management function increases the likelihood of unauthorized or inadequately reviewed changes and possible breakdowns in the system's functionality. Additionally, our review identified several instances in which OIT management failed to properly segregate the duties of employees or adequately monitor system access rights. This can lead to unauthorized and undetected changes to applications and data, increasing the risk for potential fraud and abuse within the city's financial systems. Both of these findings were included as significant deficiencies in the previous IT general controls report.

I want to urge you to address these significant deficiencies with urgency because if issues like this are not resolved, they can become bigger problems down the road. For example, both change management and segregation of duties were findings in my office's review of the OnePhilly system. As the OnePhilly review showed, weaknesses in these controls contributed to widespread problems within the OnePhilly system, including employees being paid incorrectly and inefficiencies across departments.

The findings and recommendations contained in the report were shared with management during the audit process. We believe the recommendations in the attached report, if implemented, will improve the general controls over the city's IT systems. We included management's written response to the findings and recommendations as part of the report.

We would like to express our thanks to OIT management and staff for their cooperation during the audit process.

Sincerely,

Rebecca Rhynhart
City Controller

CC: Honorable James F. Kenney, Mayor
Honorable Darrell L. Clarke, President, City Council
Honorable Members of City Council
Stephanie Tipton, Chief Administrative Officer
Rob Dubow, Finance Director
Members of the Mayor's Cabinet

CITY OF PHILADELPHIA
FISCAL YEAR 2019
ASSESSMENT AND EVALUATION OF THE OFFICE OF INNOVATION AND TECHNOLOGY'S IT GENERAL CONTROLS
EXECUTIVE SUMMARY

Why the Controller's Office Conducted the Examination

In accordance with the Philadelphia Home Rule Charter, the Office of the City Controller engaged the Mercadien Group, who retained BDO USA, LLP, to conduct an assessment of the Information Technology (IT) general controls administered by the Office of Innovation & Technology (OIT). The purpose of this assessment was to evaluate the IT general controls over key financial-related applications at OIT as part of the Office of the City Controller's audit of the City of Philadelphia's Comprehensive Annual Financial Report (CAFR) for the fiscal year ended June 30, 2019.

Report Findings

Based on the potential impact to the city's CAFR, the report identified four significant deficiencies, as well as several other deficiencies that require management's attention. Key findings include:

- As noted in previous reports, OIT management has not provided sufficient oversight of the change management function, the process that ensures changes to IT systems are properly approved and tested before the implementation of that change. Specifically, the change management policy provided by OIT did not establish clear procedures for reviewing, testing and documenting changes to the city's IT systems. A lack of oversight in the change management function increases the likelihood of unauthorized or inadequately reviewed changes. Additionally, inconsistencies in the processes for application changes can lead to delays in necessary changes and breakdowns in the system's functionality.

- Our review identified several instances in which OIT management did not properly segregate the duties of employees or adequately monitor system access rights. Failure to provide oversight of system access rights can lead to unauthorized and undetected changes to applications and data, increasing the risk for potential fraud and abuse within the city's financial systems. While OIT's policy states that IT administrators will ensure proper segregation of duties, the report found three programmers who had the ability to add, delete, and modify water revenue transaction data in the Basis2 application; four database administrators who also had systems administrator access to the FAMIS and ADPICS applications; and two database administrators who also had systems administrator access to Basis2.

What the Controller's Office Recommends

The Controller's Office has presented a number of recommendations to address the findings in this report. Some of the more significant recommendations are noted below.

We recommend OIT management strengthen its change management procedures and ensure that changes are properly reviewed, approved and tested before implementation. OIT management should implement proper segregation of duties and increase oversight of assigned system access rights.

Section

SECTION I

INDEPENDENT ACCOUNTING FIRM'S REPORT

CITY OF PHILADELPHIA - OFFICE OF THE CONTROLLER

Assessment and Evaluation of the Office of Innovation and Technology's IT General Controls

Tel: 215-564-1900
Fax: 215-563-3940
www.bdo.com

1801 Market Street,
Suite 1701
Philadelphia, PA19107

Rebecca Rhynhart
City Controller
City of Philadelphia
1401 JFK Boulevard, 12th Floor
Philadelphia, Pennsylvania 19102

We have concluded our engagement to perform an assessment of the Information Technology (IT) general controls implemented by the City of Philadelphia's Office of Innovation and Technology (OIT). Our engagement to perform these procedures was conducted as a consulting services engagement. This engagement was agreed to by the City of Philadelphia – Office of the Controller (Controller's Office) and was applied solely to assist you in evaluating the IT general controls of applications at the OIT as part of the city's Comprehensive Annual Financial Report audit for the year ended June 30, 2019. Management of the city is responsible for the operations of, and internal controls, over IT. We performed this engagement in accordance with Statements on Standards for Consulting Services issued by the American Institute of Certified Public Accountants. The sufficiency of the scope and procedures of our engagement is solely the responsibility of the management of the Controller's Office. Consequently, we make no representations regarding the sufficiency of the scope and procedures described in the attached document either for the purpose for which this report has been requested or for any other purpose.

We have attached observations and recommendations regarding IT general controls resulting from the consulting engagement for the consideration of the Controller's Office and OIT.

We were not engaged to, and did not perform an audit or an examination, the objective of which would be the expression of an opinion on the operations or internal controls of the OIT. Accordingly, we do not express such an opinion. Had we performed additional procedures, other matters might have come to our attention that would have been reported to you.

The procedures performed and related observations and recommendations are described in the attached document. We performed our procedures during the months of September 2019 through January 2020.

This report is intended solely for the use of the management of the Controller's Office and the OIT and should not be used by others.

BDO USA, LLP

BDO USA, LLP

Philadelphia, Pennsylvania
January 7, 2020

City of Philadelphia – Office of the Controller
Assessment and Evaluation of the
Office of Innovation and Technology's IT General Controls
As of June 30, 2019

Table of Contents

City of Philadelphia – Office of the Controller
Assessment and Evaluation of the
Office of Innovation and Technology's IT General Controls
As of June 30, 2019

Executive Summary

The Office of the Controller (Controller's Office) engaged BDO USA, LLP (BDO), with the assistance of the Mercadien Group, to perform an assessment of Information Technology (IT) general controls related to the City of Philadelphia's Office of Innovation and Technology's (OIT's) operations.

We conducted this engagement in accordance with Statements on Standards for Consulting Services issued by the American Institute of Certified Public Accountants. The scope of the review included the internal controls in place as of June 30, 2019.

Summary of Objective, Scope and Methodology

The objective of the BDO consulting engagement was to provide an assessment and evaluation of the IT general controls implemented by the City of Philadelphia's OIT in support of the Controller's Office audit of the city's Comprehensive Annual Financial Report (CAFR). The scope of the review included the internal controls in place as of June 30, 2019. Our engagement was structured to address the following five (5) areas as requested by the Controller's Office:

1. *Security Management* - the controls designed and placed into operation to provide reasonable assurance that security management is effective.

2. *Configuration Management* - the controls designed and placed into operation to provide reasonable assurance that changes to information system resources are authorized and systems are configured and operated securely and as intended.

3. *Segregation of Duties* - the controls designed and placed into operation to provide reasonable assurance that incompatible duties are effectively segregated.

4. *Access Controls and System Files* - the controls designed and placed into operation to provide reasonable assurance that access to computer resources (data, equipment, and facilities) is reasonable and restricted to authorized individuals.

5. *Contingency Planning* - the controls designed and placed into operation to provide reasonable assurance that contingency planning (a) protects information resources and minimizes the risk of unplanned interruptions and (b) provides for recovery of critical operations should interruptions occur.

The following applications were included in the scope of our work:

- Financial Accounting Management Information System (FAMIS)
- Advanced Purchasing Inventory Control System (ADPICS)
- Payroll (through March 18, 2019 when replaced by OnePhilly)
- Pension Payroll
- Health and Welfare (through December 17, 2018 when replaced by OnePhilly)
- Taxpayer Inquiry and Payment System (TIPS)
- Basis2 (i.e. the city's water billing system)

Summary of Observations

Below we are providing a summary of our key observations noted through the procedures performed for this engagement. Based upon its potential impact on the city's CAFR, each key finding listed below was assigned a rating of either Material Weakness or Significant Deficiency.[1] Additional details for these key observations as well as other observations with low impact (rated as Deficiency) are provided in the detailed section of our report.

Area	Findings	Potential Impact
Security Management	Control deficiencies were noted for this area, but none were deemed to be a material weakness or significant deficiency.	N/A
Configuration Management	1. Change requests were not consistently supported by documented end-user testing or management approval, including evidence of review and approval by the Change Advisory Board.	Significant Deficiency
	2. Three OIT programmers have development rights to Basis2 as well as database administrator access rights.	Significant Deficiency
Segregation of Duties	3. Four OIT database administrators have systems administrator access within FAMIS and ADPICS, creating a segregation of duties risk.	Significant Deficiency
	4. Two OIT database administrators have systems administrator access within Basis2, creating a segregation of duties risk.	Significant Deficiency
Access Controls and System Files	Control deficiencies were noted for this area, but none were deemed to be a material weakness or significant deficiency.	N/A
Contingency Planning	Control deficiencies were noted for this area, but none were deemed to be a material weakness or significant deficiency.	N/A

[1] The AICPA's *Professional Standards (Clarified)* AU-C Section 265.07 states that 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. AU-C Section 265.07 provides the following definitions:
Material Weakness – This 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.
Significant Deficiency – This 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.

Detailed Results

Objective, Scope and Methodology

The objective of the BDO consulting engagement was to provide an assessment and evaluation of the IT general controls implemented by the OIT in support of the Controller's Office audit of the city's CAFR. Our engagement was structured to address the five (5) areas as outlined in our proposal. Within each area, we focused on several control elements as follows:

OUR MAJOR CONCENTRATION WILL FOCUS ON THE APPLICATION OF THE FOLLOWING:	
Security Management	• Periodic assessments and validation of risk • Security control policies and procedures • Security awareness training and other security related personnel issues • Periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices • Remediation of information security weaknesses • Security over activities performed by external third parties
Configuration Management	• Configuration management policies, plans, and procedures • Current configuration identification information • Proper authorization, testing, approval, and tracking of all configuration changes • Routine monitoring of the configuration • Updating software on a timely basis to protect against known vulnerabilities • Documentation and approval of emergency changes to the configuration
Segregation of Duties	• Segregation of incompatible duties and responsibilities and related policies • Control of personnel activities through formal operating procedures, supervision, and review
Access Controls and System Files	• Protection of information system boundaries • Identification and authentication mechanisms • Authorization controls • Protection of sensitive system resources • Audit and monitoring capability, including incident handling • Physical security and environmental controls
Contingency Planning	• Protection of information resources and minimizing the risk of unplanned interruptions • Provision for recovery of critical operations should interruptions occur, including effective: - Assessment of the criticality and sensitivity of computerized operations and identification of supporting resources; - Steps taken to prevent and minimize potential damage and interruption; - Comprehensive contingency plan; and - Periodic testing of the contingency plan, with appropriate adjustments to the plan based on testing.

Background Information on OIT

OIT's Mission Statement

OIT's mission is to align information technology in support of the business of city government and to manage the city's technology assets efficiently and effectively. In this way, the City of Philadelphia will become a more agile and innovative organization that is better able to improve services to all Philadelphians.

Establishment of OIT and Its Responsibilities and Services

OIT was established in August 2011 by Mayor's executive order. OIT oversees all major information and communications technology initiatives for the City of Philadelphia. OIT's main responsibilities include:

- Identifying the most effective approach for implementing new information technology directives throughout city government.
- Improving the value of the city's technology assets and the return on the city's technology investments.
- Ensuring data security and continuity.
- Planning for continuity operations in the event of disruption of information technology or communications services.
- Supporting accountable, efficient, and effective government across every city department, board, commission, and agency.

OIT's seven major service areas are described below.

Automated and Digital Government – Services which automate and simplify business processes and workflow and provide easy-to-use business intelligence tools.

- Cultural and Natural Resources Applications
- Economic Development Applications
- Enterprise Application Services
- Enterprise Database, Storage, Platform and Hosting
- Financial Applications
- Human Capital Management
- Legal Applications
- Public Safety Applications
- Transportation and Utilities Applications
- Web Presence Management
- Enterprise Geodata Management and Map Services

Business Protection – Services that protect the continuity of the city's business operations, and the confidentiality of the city's assets, systems, data and employee privacy.

- Business Continuity
- Information Security
- Risk Management

Collaboration & Communication – Services which enable staff and consultants to share information and work together in an effective, efficient manner on tasks, projects and initiatives.

- Dispatch

- Email
- Enterprise Voice
- Instant Messaging
- Media and Events
- Mobile Communication Management
- Video Conferencing
- Enterprise and Public Web Mapping

Connectivity – Services which allow staff to access IT resources for local and remote sites and share information with business partners.

- On-Premise Access
- Remote Access
- Wireless Access

Innovation and Open Government – Services which make technology and information accessible and useful to Philadelphians and their communities and provide an innovation infrastructure to solve urban challenges in new ways.

- Digital Inclusion and Access
- Innovation Governance and Management
- Enterprise and Open Data Publishing
- Geodata Analysis and Visualizations

Professional Services – Professional services which focus on planning, governing and managing IT investments, people and technologies to increase alignment with the business.

- Project Management
- Technology and Strategy Planning
- Vendor and Contract Management

Technology and User Support – Services which support various end-user technology resources, needs and requests.

- Account Management
- Desktop Management
- File and Print Management
- Service Center
- End User Device Management

RESULTS

Observations

Below is our summary of key observations noted through the procedures performed for this engagement. Our observations include the details of the condition, criteria, related effect/risk, cause, our recommendation, and the potential impact.

Security Management

1. IT Risk Assessment

   Condition: As previously reported, the OIT has not yet performed a comprehensive IT risk assessment. While the OIT does have a process to monitor technical risks through vulnerability scanning, a formal plan to identify and address additional IT operational, business and compliance risks does not exist.

   Criteria: The OIT's Information Security Governance Policy states that City governance functions that provide strategic direction for information security should manage risks appropriately. An IT risk assessment helps management understand what events can affect its entity in a negative way and what security gaps pose a threat to critical information so management can make better security decisions and take proactive measures.

   Effect/Risk: Without a current and comprehensive risk assessment, IT resources may be used ineffectively in addressing risk affecting OIT.

   Cause: OIT completed the first step of the process in having a Cybersecurity risk assessment completed in 2019, but has not completed the formal IT risk assessment.

   Recommendation: OIT should develop formal procedures to perform periodic risk assessments and monitor gaps identified. This should be a component of an enterprise wide risk management program [300413.01].

   Potential Impact: **Deficiency**

2. IT Policies and Procedures – Basis2 Security Policy

   Condition: As of the end of our fieldwork, the Revenue IT group[2] did not provide a documented security policy that governs the Basis2 application. This condition was also noted in the prior review.

   Criteria: A written information security policy is essential to establish and communicate to all users the rules and procedures to be followed in accessing and using an application and its data.

   Effect/Risk: Failure to formally develop and document security policies and procedures increases the risk that critical control activities for monitoring security threats may be inconsistently applied. As a result, the Basis2 application is at an increased risk for data leak and/or loss.

   Cause: OIT has not made it a priority to work with the Basis2 application owners to finalize a security policy.

   Recommendation: OIT should work with the Basis2 application owners to establish

[2] The Revenue IT group, which consists of assigned employees from OIT, administers both Basis2 and TIPS for the Revenue Department.

and disseminate to users a formal security policy for the Basis2 application. Once the policy is established, OIT should periodically review it to determine if it requires updating [300416.01].

Potential Impact: **Deficiency**

3. IT Policies and Procedures – Firewall Administration, Maintenance, and Monitoring
Condition: OIT's existing documented policies do not cover firewall administration, maintenance, and monitoring requirements.

Criteria: An entity must establish firewall policies to ensure that it has adequate monitoring of all the data passing in and out of the network to keep out malicious users and programs.

Effect/Risk: Failure to formally develop and document security policies and procedures around firewall management and maintenance standards increases the risk of security exposure, security breaches, and unauthorized external access to applications and data.

Cause: OIT management has not updated its existing written policies to incorporate firewall management standards and monitoring requirements.

Recommendation: OIT should update the Information Security Access Control Policy and the Information Security Operations Management Policy to include details of the firewall management standards and the required firewall maintenance monitoring [300419.01].

Potential Impact: **Deficiency**

Configuration Management

4. Application Change Management
Condition: The current change management policy provided by OIT management does not specifically address (1) details on the Change Advisory Board (CAB) approval process that our prior review noted as having been added to the policy and (2) how end-user testing should be documented. OIT management indicated that they are working on an updated change management policy, which will address the CAB approval process and documentation of end-user testing. Additionally, the policy does not clearly identify the level of approvals required for the different types of changes that are migrated to production.

As noted in prior reviews, the procedure was still inconsistently applied when performing change requests for in-scope applications. Change requests sampled by us were not consistently supported by documented end-user testing, including detailed testing procedures, and identification that testing was completed. Also, for sampled change requests, the service tickets did not consistently document required approvals, including evidence of review and approval by the CAB.

Criteria: Change management procedures should establish clear performance and documentation standards for end-user testing and required approvals to ensure that requested application changes are adequately tested and properly approved before migration to production.

Effect/Risk: Inadequate compliance with established procedures to perform end-user

testing and management approval increases the possibility that unauthorized or inadequately reviewed changes will be implemented in the production environment.

Cause: OIT management has not performed sufficient oversight of the change management function to ensure that established procedures are routinely followed and that the policy clearly identifies standards for documenting end-user testing and the required approvals (including CAB) for the different change types.

Recommendation: OIT should review its change control procedures and implement measures to ensure that required steps for application changes are performed and documented in accordance with the policy. Also, OIT should update its change management policy to include (1) documentation standards for end-user testing and (2) more detail related to required approvals for all change types and how those approvals should be documented in the service ticket [300413.05].

Potential Impact: **Significant Deficiency**[3]

5. Developers with Database Administrator Access Rights – Basis2
Condition: Three OIT programmers have development rights to Basis2 as well as database administrator access rights.

Criteria: OIT's Information Security Administrator Acceptable Use Policy Section 5.1.1 states that IT administrators shall ensure that information systems are configured to provide the ability for segregation of duties to reduce potential damage from the actions of one person. For example, responsibility for initiating transactions, recording transactions and custody of information systems on which the transactions have been performed are assigned to separate individuals.

Effect/Risk: With the combination of (a) developer access rights, which allows for the creation or modification of code, configuration, and data, along with (b) the database administrator's ability to make direct data changes to the database tables, there is an increased risk for unauthorized and improper code migrations, configuration changes, and data changes occurring without detection.

Cause: OIT management did not exercise sufficient oversight of system access rights assigned to the three programmers to ensure separation of development rights from database administrator access or, if segregation of duties was not feasible, that there was monitoring of the programmers' activities.

Recommendation: For the three programmers, OIT should separate the developer/programmer function from the database administrator function. If segregation of duties is not feasible, OIT should monitor the activities of the three programmers to ensure they are authorized and appropriate [300419.02].

Potential Impact: **Significant Deficiency**

Segregation of Duties

6. Database Administrator and Systems Administrator Access – FAMIS and ADPICS
Condition: Four OIT employees have database administrator access as well as systems administrator access within FAMIS and ADPICS, creating a segregation of

[3] In determining the Significant Deficiency rating for the change management finding, we identified and evaluated manual compensating controls that would mitigate the impact on the city's CAFR.

duties risk.

Criteria: OIT's Information Security Administrator Acceptable Use Policy Section 5.1.1 states that IT administrators shall ensure that information systems are configured to provide the ability for segregation of duties to reduce potential damage from the actions of one person. For example, responsibility for initiating transactions, recording transactions and custody of information systems on which the transactions have been performed are assigned to separate individuals.

Effect/Risk: With the combination of (a) systems administrator access rights, which allows for the creation or modification of user rights to perform transactions or change system configurations, along with (b) the database administrator's ability to make direct data changes to the database tables, there is an increased risk for unauthorized and improper data changes occurring without detection.

Cause: OIT management did not adequately monitor the access rights assigned to these four employees to ensure separation of systems administrator access from database administrator access or, if segregation of duties was not feasible, that there was monitoring of these employees' activities.

Recommendation: For these four employees, OIT should separate the systems administrator function from the database administrator function. If segregation of duties is not feasible, OIT should monitor the activities of these employees to ensure they are authorized and proper [300419.03].

Potential Impact: **Significant Deficiency**

7. Database Administrator and Systems Administrator Access – Basis2

Condition: Two OIT employees have database administrator access as well as systems administrator access within Basis2, creating a segregation of duties risk.

Criteria: OIT's Information Security Administrator Acceptable Use Policy Section 5.1.1 states that IT administrators shall ensure that information systems are configured to provide the ability for segregation of duties to reduce potential damage from the actions of one person. For example, responsibility for initiating transactions, recording transactions and custody of information systems on which the transactions have been performed are assigned to separate individuals.

Effect/Risk: With the combination of (a) systems administrator access rights, which allows for the creation or modification of user rights to perform transactions or change system configurations, along with (b) the database administrator's ability to make direct data changes to the database tables, there is an increased risk for unauthorized and improper data changes occurring without detection.

Cause: OIT management did not perform sufficient oversight of access rights assigned to these two employees to ensure separation of systems administrator access from database administrator access or, if segregation of duties was not feasible, that there was monitoring of these employees' activities.

Recommendation: For these two employees, OIT should separate the systems administrator function from the database administrator function. If segregation of duties is not feasible, OIT should monitor the activities of these employees to ensure they are authorized and appropriate [300419.04].

Potential Impact: **Significant Deficiency**

Access Controls and System Files

8. Authorization – Database Administrator Access

Condition: As previously reported, the OIT was unable to provide evidence documenting the authorization of database access for four IT consultants functioning as database administrators for Basis2.

Criteria: OIT's Information Security Access Control Policy (updated effective June 21, 2019) Section 7 requires that all information users must be authorized before gaining access to any city system. Section 7.1 of this policy states that OIT's Information Security Group and information owners must ensure that all special or privileged access to systems (such as administrative or supervisor accounts) are reviewed quarterly, and any changes to privileged accounts must be logged and periodically reviewed.

Effect/Risk: Unauthorized access to the database could lead to unapproved or inappropriate database activities and/or direct data table changes.

Cause: OIT has not established a formal written policy for the authorization of system access for consultants. In previous audits, OIT management provided a draft policy setting forth a process for the granting of database system access to IT consultants and informed us they were developing a form for the request and approval of Basis2 access. However, during the current review, OIT did not provide us with the finalized, formally approved versions of this policy and form.

Recommendation: OIT management should finalize and formally approve the policy for granting of database system access to IT consultants and the Basis2 access request form. This policy should require that, when granting access to consultants, OIT:

- Maintain the authorizing documentation for all users granted access.
- Obtain and review the consultant's contract and confirm with the supervising manager that the consultant's access is appropriate.
- Check periodically with the supervising manager that access is still appropriate, authorized, and supported by an active vendor contract [300416.04].

Potential Impact: **Deficiency**

9. Periodic Access Rights Review

Condition: As previously reported, OIT was still unable to provide evidence that periodic reviews of active users' access rights had been completed for all in-scope applications.

Criteria: OIT's Information Security Access Control Policy (updated effective June 21, 2019) Section 7.1 states that information owners are responsible for reviewing system privileges on a periodic basis (quarterly at a minimum) and must promptly revoke or amend privileges no longer required by users. Also, this policy requires that (a) information owners and OIT's Support Center must ensure that privileges assigned to employees transferring or changing job responsibilities are reviewed and re-allocated as determined by their new role and (b) OIT's Information Security Group and information owners must ensure that all special or privileged access to systems (such as administrative or supervisor accounts) are reviewed quarterly, and any changes made to privileged accounts must be logged and periodically reviewed.

Effect/Risk: There is a risk that over time access rights will not be updated due to oversights.

Cause: Application owners did not formally complete access rights reviews and document the results of the review. In certain instances, application owners appeared to be relying on the 30-day inactive list process as the recertification review, but this did not cover a review of application responsibilities assigned.

Recommendation: OIT should work with the impacted departments to complete the required reviews of the active users and their associated access rights for appropriateness [300416.05].

Potential Impact: **Deficiency**

10. User Administration – Notification of Terminated Users

Condition: For 2 of 8 terminated employees sampled, OIT was unable to provide evidence documenting the notification to OIT's Support Center and IT Administrators requesting removal of access rights to the network and in-scope applications. For all terminated employees sampled, we noted that access to the network and all in-scope applications was properly removed. This condition was also noted in the prior review.

Criteria: OIT's Information Security Access Control Policy (updated effective June 21, 2019) Section 7.3 states that the city must implement specific procedures to ensure that inactive accounts are disabled or deleted in a timely manner, and the OIT's Support Center must ensure that inactive user accounts are disabled within 7 days of termination.

Effect/Risk: Without evidence of notification of termination to management and owners of applications, users may retain access beyond their termination date resulting in the possible unauthorized use of these accounts.

Cause: OIT had not established a formally documented process for the notification of employee terminations to OIT's Support Center and IT Administrators.

Recommendation: OIT should work with the Office of Human Resources and/or OnePhilly Team to establish a formally documented process for the notification of employee terminations to OIT's Support Center and IT Administrators. Established procedures should include formal documentation requirements for notifications, including retention of those notifications so they are available for later review and audit [300416.07].

Potential Impact: **Deficiency**

Contingency Planning

11. Business Continuity Plan

Condition: As previously reported, a business continuity plan has not yet been developed for the in-scope applications.

Criteria: Business continuity plans are vital to organizations so they have a proactive plan to avoid and mitigate risks associated with unplanned disruptions of operations.

Effect/Risk: In the event of a disruption of service, city departments may not be able to provide required services or continue limited operations until service is restored.

Cause: OIT has noted its Continuity of Operations Program (COOP) plan is not based on current information and needs updating. While OIT management acknowledged it would be beneficial to obtain all departments' COOP plans so OIT could advise them on the adequacy of the plan's IT component, they stated that the Office of Emergency Management (OEM) was responsible for coordinating the COOP program and obtaining the departments' plans.

Recommendation: OIT management should request the assistance of OEM in obtaining the departments' COOP plans so OIT could review the IT components of the plans. OIT should provide guidance and assistance in helping the impacted departments when establishing the plans. Also, OIT should update its own COOP plan based on current information [300413.13].

Potential Impact: **Deficiency**

12. Basis2 Disaster Recovery

Condition: As noted in the prior report, there was no formal written disaster recovery plan that specifically addressed Basis2.

Criteria: Disaster recovery is an essential area of security planning that aims to protect an entity from the effects of significant negative events. It is a plan for restoring and accessing an entity's data in the event of a disaster that destroys part or all of an entity's resources and allows an entity to maintain or quickly resume critical functions following a disaster.

Effect/Risk: In the event of a disruption of service, the city may not be able to provide required services or continue limited operations until service is restored.

Cause: Management asserted there were disaster recovery procedures in place for Basis2 with the Basis2 database automatically copied to a tape unit on a weekly basis and the backup's integrity automatically tested for validity by the Commvault backup system. Although these procedures indicate information and data is available for recovery, this is not a documented disaster recovery plan and is not evidence of an annual recovery test.

Recommendation: OIT management should develop a formal written disaster recovery plan that specifically addresses Basis2. Once established, OIT should periodically (at least annually) test the plan and document the tests and their results in writing [300413.14].

Potential Impact: **Deficiency**

REMEDIATION OF PRIOR REPORTED FINDINGS

As part of this engagement, we also followed up on the remediation status of control weaknesses noted by the Controller's Office in prior reviews of OIT's IT general controls. Several previously reported conditions remained uncorrected and were discussed in the preceding section of this report. These uncorrected prior year conditions involved the OIT's failure to perform a comprehensive IT risk assessment; the lack of a Basis2 security policy; change management procedures not being consistently followed; no evidence for authorization of database access for IT consultants functioning as Basis2 database administrators; no evidence of periodic access rights reviews; failure to send notifications for terminated users; the lack of formal business continuity plans; and no disaster recovery plan for Basis2.

Our testing found that the following prior-noted conditions were resolved:

Access Controls and System Files

User Administration - New Hires

Condition: Prior audit testing of new hires found that OIT was unable to provide evidence documenting the request authorizing that the new hire be granted access to the Active Directory or the in-scope applications.

Remediation Status: **Complete** – OIT's Information Security Access Control Policy was updated on June 21, 2019 with requirements for authorization of access requests. Sample testing of new hires during the fiscal 2019 review did not identify any issues with new hire authorization and accuracy of access granted [300416.06].

Contingency Planning

Disaster Recovery Plan and Testing

Condition: The prior audit disclosed that OIT was working on the development of a formal disaster recovery plan for enterprise IT operations. Also, the prior review noted a lack of involvement of city departments in the disaster recovery testing. OIT did not have a process in place to ensure that city departments were sufficiently testing their applications during the recovery process.

Remediation Status: **Complete** – During the current review, OIT provided a formal disaster recovery plan for enterprise IT operations (except for Basis2 as noted in finding number 12 above). In the recent annual disaster recovery test completed on November 26, 2019, there was a plan for involvement of city departments, and city department involvement was not noted as an issue [300416.10].

SECTION II

MANAGEMENT'S RESPONSE

CITY OF PHILADELPHIA
Office of Innovation & Technology

Mark Wheeler
Chief Information Officer
1234 Market Street, Suite 1800
Philadelphia, PA 19107
Phone: (215) 686-5912
Fax: (215) 686-8258

May 22, 2020

Honorable Rebecca Rhynhart
City Controller
1230 Municipal Services Building
1401 John F. Kennedy Boulevard
Philadelphia, PA 19102-1679

Re: Draft Report - Assessment and Evaluation of the Office of Innovation and Technology's IT General Controls Control – Fiscal 2019

Dear Ms. Rhynhart:

Thank you for the opportunity to respond to the findings and recommendations included in the above-referenced draft report ("the Report"). Also, we extend our thanks and appreciation to your audit team and the representatives of BDO USA, LLP, who consistently worked cooperatively with the Office of Innovation and Technology ("OIT") to complete the assessment of the information technology general controls related to OIT's operations.

We offer the following responses to the conditions and recommendations noted in the Report.

Security Management

1. IT Risk Assessment

Condition: As previously reported, the OIT has not yet performed a comprehensive IT risk assessment. While the OIT does have a process to monitor technical risks through vulnerability scanning, a formal plan to identify and address additional IT operational, business and compliance risks does not exist.

Recommendation: OIT should develop formal procedures to perform periodic risk assessments and monitor gaps identified. This should be a component of an enterprise wide risk management program [300413.01].

Response: OIT is committed to maintaining a secure environment across all city systems and proactively identifying and promptly mitigating risks and potential security threats. As such, OIT shall continue to develop and implement formal procedures that institutionalize periodic risk assessments. To that end, in 2019 OIT engaged a consultant to conduct an Enterprise IT Operations Gap Analysis. This analysis examined specific operational areas that underwent a review of existing controls in order to identify material weaknesses. The Gap Analysis was completed at the end of 2019 and several action plans were presented to OIT, including a plan to develop procedures and policies supporting regular assessments to identify and address compliance risks. When the City resumes normal operations, OIT will begin executing on the presented action plans.

2. IT Policies and Procedures – Basis2 Security Policy

Condition: As of the end of our fieldwork, the Revenue IT group did not provide a documented security policy that governs the Basis2 application. This condition was also noted in the prior review.

Recommendation: OIT should work with the Basis2 application owners to establish and disseminate to users a formal security policy for the Basis2 application. Once the policy is established, OIT should periodically review it to determine if it requires updating [300416.01].

Response: Although a general security policy exists, OIT recognizes the need to finalize a security policy that specifically governs the Basis2 application. One outcome of the Enterprise IT Operations Gap Analysis noted above is the creation of several action plans presented to OIT, including one for following a NIST-based process for the development, updating, finalization and implementation of security policies. When the City resumes normal operations, OIT will begin executing on the presented action plans.

3. IT Policies and Procedures – Firewall Administration, Maintenance, and Monitoring

Condition: OIT's existing documented policies do not cover firewall administration, maintenance, and monitoring requirements.

Recommendation: OIT should update the Information Security Access Control Policy and the Information Security Operations Management Policy to include details of the firewall management standards and the required firewall maintenance monitoring [300419.01]

Response: OIT recognizes the need to update the noted security policies. An action plan presented to OIT as an outcome of the 2019 Enterprise IT Operations Gap Analysis includes a NIST-based process for the development, updating, finalization and implementation of security policies. When the City resumes normal operations, OIT will begin executing on the presented action plans.

Configuration Management

4. Application Change Management

Condition: The current change management policy provided by OIT management does not specifically address (1) details on the Change Advisory Board (CAB) approval process that our prior review noted as having been added to the policy and (2) how end-user testing should be documented. OIT management indicated that they are working on an updated change management policy, which will address the CAB approval process and documentation of end-user testing. Additionally, the policy does not clearly identify the level of approvals required for the different types of changes that are migrated to production.

As noted in prior reviews, the procedure was still inconsistently applied when performing change requests for in-scope applications. Change requests sampled by us were not consistently supported by documented end-user testing, including detailed testing procedures, and identification that testing was completed. Also, for sampled change requests, the service tickets did not consistently document required approvals, including evidence of review and approval by the CAB.

Recommendation: OIT should review its change control procedures and implement measures to ensure that required steps for application changes are performed and documented in accordance with the policy. Also, OIT should update its change management policy to include (1) documentation standards for end-user testing and (2) more detail related to required approvals for all change types and how those approvals should be documented in the service ticket [300413.05].

Response: OIT recognizes the importance of overseeing change control procedures and ensuring that application changes are conducted in accordance with policy. OIT will continue to review its change control procedures and implement measures to ensure that the process is adhered to for application changes. And, as an integral part of that oversight, OIT also acknowledges the need to make certain that the change management policy is updated to include necessary and appropriate controls. OIT will work to revise its change management policy to include the two additional recommended requirements.

5. Developers with Database Administrator Access Rights – Basis2

Condition: Three OIT programmers have development rights to Basis2 as well as database administrator access rights.

Recommendation: For the three programmers, OIT should separate the developer/programmer function from the database administrator function. If segregation of duties is not feasible, OIT should monitor the activities of the three programmers to ensure they are authorized and appropriate [300419.02].

Response: OIT will assess separating the noted functions and will segregate the duties associated with each among available employees where possible. Where, due to limited resources, OIT must rely on one employee to perform multiple functions, OIT will make every effort to monitor employee activity.

Segregation of Duties

6. Database Administrator and Systems Administrator Access – FAMIS and ADPICS

Condition: Four OIT employees have database administrator access as well as systems administrator access within FAMIS and ADPICS, creating a segregation of duties risk.

Recommendation: For these four employees, OIT should separate the systems administrator function from the database administrator function. If segregation of duties is not feasible, OIT should monitor the activities of these employees to ensure they are authorized and proper [300419.03].

Response: OIT will assess separating the noted functions and will segregate the duties associated with each among available employees where possible. Where, due to limited resources, OIT must rely on one employee to perform multiple functions, OIT will make every effort to monitor employee activity.

7. Database Administrator and Systems Administrator Access – Basis2

Condition: Two OIT employees have database administrator access as well as systems administrator access within Basis2, creating a segregation of duties risk.

Recommendation: For these two employees, OIT should separate the systems administrator function from the database administrator function. If segregation of duties is not feasible, OIT should monitor the activities of these employees to ensure they are authorized and appropriate [300419.04].

Response: OIT will assess separating the noted functions and will segregate the duties associated with each among available employees where possible. Where, due to limited resources, OIT must rely on one employee to perform multiple functions, OIT will make every effort to monitor employee activity.

Access Controls and System Files

8. Authorization – Database Administrator Access

Condition: As previously reported, the OIT was unable to provide evidence documenting the authorization of database access for four IT consultants functioning as database administrators for Basis2.

Recommendation: OIT management should finalize and formally approve the policy for granting of database system access to IT consultants and the Basis2 access request form. This policy should require that, when granting access to consultants, OIT:

- Maintain the authorizing documentation for all users granted access.
- Obtain and review the consultant's contract and confirm with the supervising manager that the consultant's access is appropriate.
- Check periodically with the supervising manager that access is still appropriate, authorized, and supported by an active vendor contract [300416.04].

Response: OIT recognizes the importance of overseeing procedures for granting database access and ensuring that such access for consultants is carefully monitored. OIT will continue to work on finalizing and approving a database access policy with the necessary and appropriate controls, including the recommended requirements.

9. Periodic Access Rights Review

Condition: As previously reported, OIT was still unable to provide evidence that periodic reviews of active users' access rights had been completed for all in-scope applications.

Recommendation: OIT should work with the impacted departments to complete the required reviews of the active users and their associated access rights for appropriateness [300416.05].

Response: OIT will increase its efforts working with departments to ensure that active user access reviews are completed periodically, and user access rights are level-set as necessary.

10. User Administration – Notification of Terminated Users

Condition: For 2 of 8 terminated employees sampled, OIT was unable to provide evidence documenting the notification to OIT's Support Center and IT Administrators requesting removal of access rights to the network and in-scope applications. For all terminated employees sampled, we noted that access to the network and all in-scope applications was properly removed. This condition was also noted in the prior review.

Recommendation: OIT should work with the Office of Human Resources and/or OnePhilly Team to establish a formally documented process for the notification of employee terminations to OIT's Support Center and IT Administrators. Established procedures should include formal documentation requirements for notifications, including retention of those notifications so they are available for later review and audit [300416.07].

Response: OIT teams have already engaged with the OnePhilly Team to address a reporting process for updated and as near real-time notification of employee separations. The teams will continue to work together to formally document the reporting process and establish a method to retain notifications.

Contingency Planning

11. Business Continuity Plan

Condition: As previously reported, a business continuity plan has not yet been developed for the in-scope applications.

Recommendation: OIT management should request the assistance of OEM in obtaining the departments' COOP plans so OIT could review the IT components of the plans. OIT should provide guidance and assistance in helping the impacted departments when establishing the plans. Also, OIT should update its own COOP plan based on current information [300413.13].

Response: As part of its preparation for maintaining operations during the City's response to the recent COVID 19 pandemic, OIT updated its COOP. OIT will continue to coordinate with OEM in their efforts assisting city departments with developing their respective COOPs and will provide guidance and assistance as necessary with any IT components of each plan.

12. Basis2 Disaster Recovery

Condition: As noted in the prior report, there was no formal written disaster recovery plan that specifically addressed Basis2.

Recommendation: OIT management should develop a formal written disaster recovery plan that specifically addresses Basis2. Once established, OIT should periodically (at least annually) test the plan and document the tests and their results in writing [300413.14].

Response: OIT recognizes the need for a documented and periodically tested disaster recovery plan for all city systems and specifically for Basis2. When the City resumes normal operations, OIT will continue its work providing for disaster recovery protocols for all city systems.

Thank you for the observations provided in your Report and for the opportunity to respond. If you or your team have any questions, please feel free to contact me.

We look forward to continued cooperation with your office.

Sincerely,

DocuSigned by:
Mark Wheeler
66BC949C6B914DB...

Mark Wheeler
Chief Information Officer

cc: Stephanie Tipton, Chief Administrative Officer
Rob Dubow, Director of Finance
Kathleen Duggan, Audit Director, City Controller's Office
Christy Brady, Post-Audit Deputy Controller, City Controller's Office
Kellan White, First Deputy Controller, City Controller's Office
Sandra Carter, Deputy CIO / Chief Operating Officer
Steven Robertson, Deputy CIO / Chief of Staff
Mervisa Johnson, Director of Compliance and Internal Controls