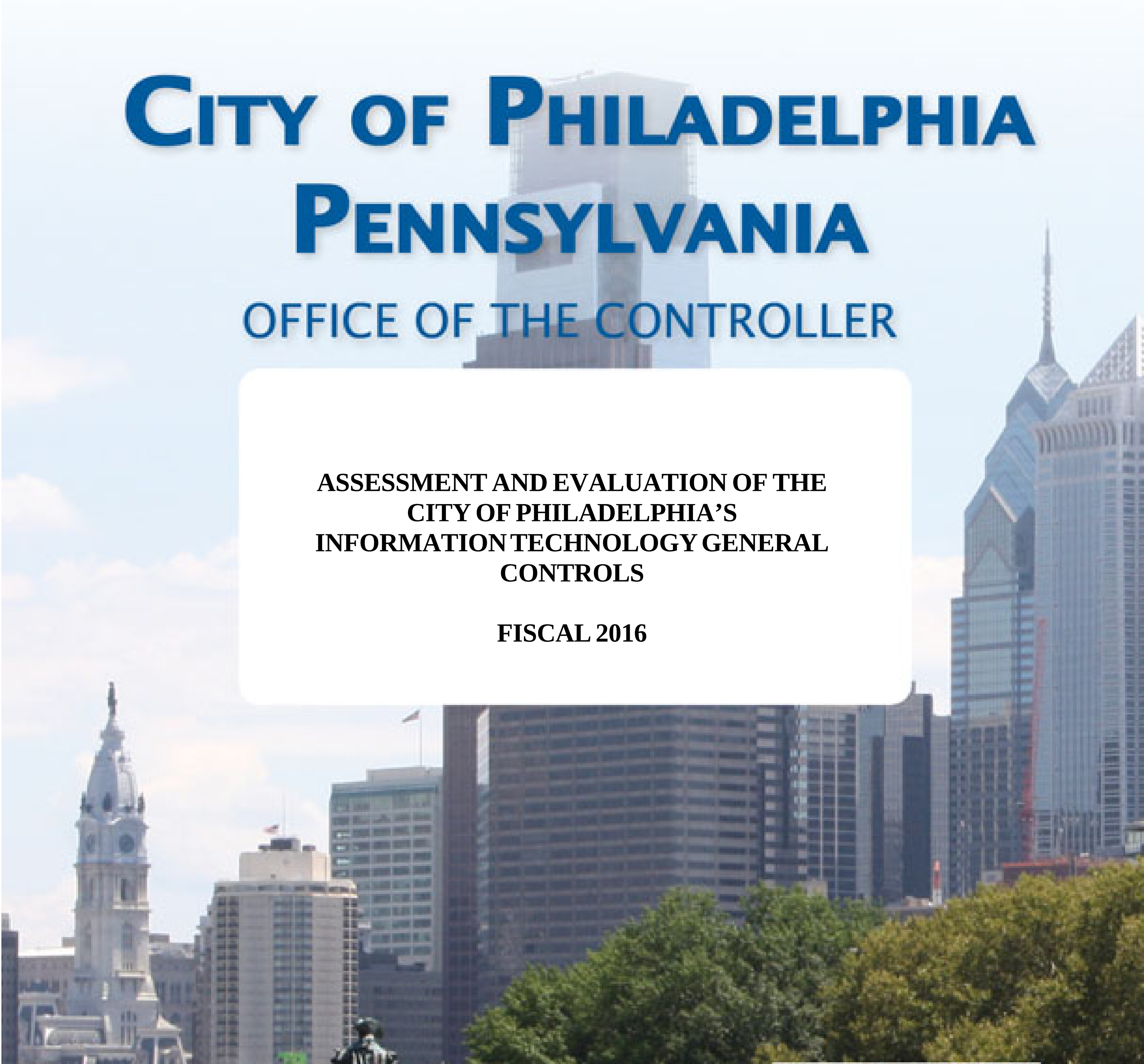
CITY OF PHILADELPHIA PENNSYLVANIA

OFFICE OF THE CONTROLLER



ASSESSMENT AND EVALUATION OF THE CITY OF PHILADELPHIA'S INFORMATION TECHNOLOGY GENERAL CONTROLS

FISCAL 2016

City Controller

Alan Butkovitz

Promoting honest, efficient & fully accountable government

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

ALAN BUTKOVITZ
City Controller

CHRISTY BRADY
Deputy City Controller

June 12, 2017

Charles J. Brennan
Chief Information Officer
Office of Innovation and Technology
1234 Market Street, Suite 1850
Philadelphia, PA 19107

Dear Mr. Brennan:

The Office of the Controller commissioned and oversaw an assessment, conducted by the independent accounting firm of BDO USA, LLP, of the information technology general controls implemented by the Office of Innovation and Technology. The purpose of this assessment was to assist my office in evaluating information technology general controls over key financial-related applications at the Office of Innovation and Technology, as part of our audit of the City's Comprehensive Annual Financial Report for the year ended June 30, 2016. The results of the independent accounting firm's assessment are summarized in the executive summary attached to this report.

We discussed the findings and recommendations with your staff at an exit conference and included your written response to the findings and recommendations in Section II of the report. We believe the recommendations in the attached report, if implemented, will improve the general controls over the city's information technology system.

We would like to express our thanks to you and your staff for the courtesy and cooperation displayed during the conduct of our work.

Very truly yours,

ALAN BUTKOVITZ
City Controller

cc: Honorable James F. Kenney, Mayor
Honorable Darrell L. Clarke, President
And Honorable Members of City Council
Rob Dubow, Director of Finance and other
Members of the Mayor's Cabinet

ASSESSMENT AND EVALUATION
OF THE CITY OF PHILADELPHIA'S
INFORMATION TECHNOLOGY GENERAL CONTROLS

EXECUTIVE SUMMARY

Why the Controller's Office Conducted the Examination

Pursuant to the Philadelphia Home Rule Charter, the Controller's Office engaged BDO USA, LLP to conduct an assessment of the Information Technology (IT) general controls implemented by the Office of Innovation and Technology (OIT). The objective of this assessment was to evaluate the IT general controls over key financial-related applications at the OIT in connection with the Controller's Office audit of the City of Philadelphia, Pennsylvania's Comprehensive Annual Financial Report for the year ended June 30, 2016.

What the Controller's Office Found

Key findings in the report are listed below. We believe these findings, and others described in the report warrant the attention of management.

- Procedures requiring approval and documentation of changes to the IT system prior to migration to production were not consistently followed. Documentation for changes to the city's IT systems did not consistently evidence end-user testing or management approval. Non-compliance with approval and documentation requirements increases the likelihood of unauthorized changes to the city's IT systems.
- OIT did not properly segregate the duties of (1) two programmers who had the ability to add, delete, and modify payroll transaction data; (2) two employees with development and systems administrator access rights to three applications; and (3) a database administrator who also had systems administrator access to one application. Consequently, there was an increased risk of unauthorized and improper changes to applications and data.
- For our entire sample of twenty newly hired employees, there was no evidence available to document the request authorizing the granting of user access rights to the network or city IT systems. With no evidence that user access was authorized, there was increased potential for unauthorized and inappropriate activity.

What the Controller's Office Recommends

The city's OIT should (1) strengthen change management procedures and ensure that required documentation and approvals are obtained; (2) implement segregation of duties in the IT environment or develop monitoring controls to track users with known segregation of duties concerns; and (3) review the new hire setup process and develop a procedure to document new user access requests. These and other proposed actions are more fully described in the body of the report.

SECTION I

INDEPENDENT ACCOUNTING FIRM’S REPORT

CITY OF PHILADELPHIA - OFFICE OF INNOVATION AND TECHNOLOGY

Assessment and Evaluation of the City of Philadelphia’s IT General Controls

BDO

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

1801 Market Street,
Suite 1701
Philadelphia, PA19107

Mr. Alan Butkovitz
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 City Controller (the 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, 2016. 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 November 2016 through February 2017.

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
February 8, 2017

City of Philadelphia – Office of the City Controller
Assessment and Evaluation of the City of Philadelphia's Office of Innovation and Technology IT General Controls
As of June 30, 2016

Table of Contents

City of Philadelphia – Office of the City Controller
Assessment and Evaluation of the City of Philadelphia's Office of Innovation and Technology IT General Controls
As of June 30, 2016

Executive Summary

The City 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, 2016.

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 City Controller's Office audit of the Comprehensive Annual Financial Report (CAFR) of the city. The scope of the review included the internal controls in place as of June 30, 2016. Our engagement was structured to address the following five (5) areas as requested by the City 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
- Pension Payroll
- Health and Welfare
- 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. Two OIT employees have development rights to Pension Payroll, Health and Welfare, and TIPS as well as systems administrator access rights.	Significant Deficiency
Segregation of Duties	3. One OIT database administrator also has systems administrator access within Basis2, creating a segregation of duties risk.	Significant Deficiency
	4. Two OIT programmers have the ability to add, delete, or modify payroll transaction data.	Significant Deficiency
Access Controls and System Files	5. For our entire sample of twenty (20) new hires, there was no evidence available to document the request authorizing that the new hire be granted access to the Active Directory or the in-scope applications.	Significant Deficiency
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 City Controller's Office audit of the City of Philadelphia'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 detail of the condition, the related risk, and our recommendation.

Security Management

1. IT Risk Assessment
   Condition: As previously reported by the Controller's Office, 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.

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

   Recommendation: We recommend that OIT 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
   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.

   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.

   Recommendation: We recommend that the Revenue IT group utilize a formal security policy for the Basis2 application. Once the policy is established, the Revenue IT group should periodically review it to determine if it requires updating [300416.01].

   Potential Impact: **Deficiency**

Configuration Management

3. Application Change Management
   Condition: As noted in the prior general IT controls review, while OIT has developed a change management procedure, the procedure is still inconsistently applied when performing change requests for in-scope applications. Change requests are not consistently supported by documented end-user testing or management approval, including evidence of review and approval by the Change Advisory Board. Additionally, the procedure does not clearly identify the level of approvals required for the different types of changes that are migrated to production.

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

From a sample of 10 production changes selected from the new SYSAID Helpdesk system for the period of January 1, 2016 to December 15, 2016, we noted the following:
- For seven sampled changes, there was no evidence that testing occurred for these changes as there was no detailed test plan in the service ticket or testing evidence available.
- For four sampled changes, there was no evidence of approval prior to the migration to production.

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.

Recommendation: We recommend that OIT review 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 more detail related to required approvals for all change types [300413.05].

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

4. Developer Access Rights

Condition: Two OIT employees – a systems administrator and a database administrator – have development rights to Pension Payroll, Health and Welfare, and TIPS as well as systems administrator access rights.

Risk: Inadequate segregation of duties in access rights potentially allows for these employees to develop code, change application configurations, and process transactions within the application. Therefore, there is an increased risk of unauthorized and improper application and data changes.

Recommendation: We recommend that OIT create a proper segregation of duties by either (a) removing the two employees from either the development or systems administrator environments or (b) creating a monitoring activity for their activities performed as systems administrators [300416.02].

Potential Impact: **Significant Deficiency**

Segregation of Duties

5. Database Administrator and Systems Administrator Access

Condition: An OIT manager had database administrator access as well as systems administrator access within Basis2, creating a segregation of duties risk.

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.

[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.

Recommendation: We recommend that OIT either (a) remove the manager's systems administrator or database administrator access, or (b) implement a monitoring procedure to confirm that the manager's activities are authorized and appropriate [300416.03].

Potential Impact: **Significant Deficiency**

Remediation: Once we brought this matter to OIT's attention, OIT resolved this condition on January 30, 2017 by removing the manager's systems administrator access rights [300416.03].

6. Developer Access to Production
Condition: As previously reported by the Controller's Office, our current year review of the active users listing for the city's Payroll system revealed that two OIT programmers still have the ability to add, delete, or modify payroll transaction data. Only users – not programmers – should be responsible for transaction origination and correction.

Risk: This access creates a segregation of duties risk in that these developers could create and migrate code to production as well as make direct payroll data changes within the database. Consequently, there is increased potential for data to be erroneously added or modified and not be detected by management.

Recommendation: We recommend that OIT revise the programmers' access rights to the Payroll system so that they do not have the ability to add, delete, or modify payroll transaction data. If that option is not feasible, OIT should implement a monitoring procedure to confirm that the programmers' activities are authorized and appropriate [500115.11].

Potential Impact: **Significant Deficiency**

Access Controls and System Files

7. Authorization – Database Administrator Access
Condition: The OIT was unable to provide evidence documenting the authorization of database access for four IT consultants functioning as database administrators.

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

Recommendation: We recommend that OIT maintain evidence for all users granted access to the databases. When granting access to a consultant, OIT should obtain and review the consultant's contract and confirm with the supervising manager that the consultant's access is appropriate. Periodically, database access should be monitored to confirm that all accounts are appropriate, authorized, and supported by a new hire form or active vendor contract [300416.04].

Potential Impact: **Deficiency**

8. Periodic Access Rights Review
Condition: Although a formal written procedure has been established requiring periodic review of active application user accounts, associated access rights, and group membership, annual reviews for the seven in-scope applications have not been completed for fiscal year 2016.

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

Recommendation: We recommend that OIT, along with impacted departments, complete a review annually of the active users and their associate access rights for appropriateness [300416.05].

Potential Impact: **Deficiency**

9. Password Configurations

Condition: As noted in a prior Controller's Office review, while passwords are required for access to the network, applications, and supporting technologies, configurations could be enhanced to strengthen authentication mechanics. Password configurations are inconsistently implemented and do not always comply with established policies at the network, application, and database levels.

The OIT Security group has not performed a review of the financial systems' configurations to evaluate compliance with the established password policy.

Risk: Inadequate password configurations increase the possibility of unauthorized access to the system, including malicious or accidental data manipulation or breach of data confidentiality.

Recommendation: We recommend that OIT review the available configurations of each authentication point and evaluate strengthening the configuration [300413.09].

Potential Impact: **Deficiency**

10. User Administration - New Hires

Condition: For our entire sample of 20 new hires, 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.

Risk: Without evidence of the authorization of new users' access to the network and in-scope applications, unauthorized users could be granted access or users could be granted more access than necessary, potentially resulting in unauthorized and improper transactions being processed.

Recommendation: We recommend that OIT management review the new hire setup process and develop a procedure to document new user access requests and approvals so they can be easily retrieved for later review and audit [300416.06].

Potential Impact: **Significant Deficiency**

11. User Administration – Terminated Users

Condition: For 12 of 45 terminated employees sampled by us, OIT was unable to provide evidence documenting the notification to management or OIT requesting removal of access rights to the network and in-scope applications. For all 45 terminated employees sampled, we noted that access to the network and all in-scope applications was properly removed.

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.

Recommendation: We recommend that OIT management institute a policy establishing formal documentation requirements for notifications to remove employee access, including retention of those notifications so they are available for later review and audit [300416.07].

Potential Impact: **Deficiency**

12. User Administration – Notification of Terminated and Inactive Users

Condition: No evidence was provided to document that notifications are being sent to the Payroll, Pension Payroll, and Health and Welfare application groups to inform them of employee terminations and inactive users (i.e. those users who have not signed in to the application for a specified time period).

Risk: If notification of employee terminations and inactive users is not being sent to management and application owners, the terminated employees and inactive users may retain access, resulting in an increased risk for the unauthorized and inappropriate use of these accounts.

Recommendation: We recommend that OIT management institute a procedure requiring that automated notifications of terminated employees and inactive users be sent to the Payroll, Pension Payroll, and Health and Welfare application groups and these notifications be retained so they are available for later review and audit [300416.08].

Potential Impact: **Deficiency**

13. Wireless Network

Condition: City Revenue-Open Wireless Service profile (Municipal Free Public WIFI) is not encrypted and is behind the firewall.

Risk: An unencrypted wireless access point behind the firewall exposes the environment to risk of cyber-attack.

Recommendation: We recommend that OIT delete the access point or encrypt access points. [300416.09].

Potential Impact: **Deficiency**

Remediation: OIT resolved this condition on December 22, 2016 by deleting the City Revenue-Open Wireless Service profile [300416.09].

Contingency Planning

14. Business Continuity Plan

Condition: As previously reported by the Controller's Office, a business continuity plan has not yet been developed for the applications reviewed as part of this project.

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.

Recommendation: We recommend that OIT communicate with potentially impacted departments to convey the importance of establishing a business continuity plan. Additionally, OIT should provide guidance and assistance in helping the impacted departments when establishing the plans [300413.13].

Potential Impact: **Deficiency**

15. Basis2 Disaster Recovery

Condition: As noted in a prior Controller's Office review, testing of the disaster recovery plan for Basis2 has still not been performed.

Risk: The disaster recovery plan may not work as anticipated when faced with an unplanned outage.

Recommendation: We recommend that OIT periodically test the Basis2 disaster recovery plan and document the tests and their results in writing [300413.14].

Potential Impact: **Deficiency**

16. Disaster Recovery Testing

Condition: Our review noted a lack of involvement of city departments in the disaster recovery testing. OIT does not have a process in place to ensure that city departments are sufficiently testing their applications during the recovery process. Out of the five departments notified by OIT to test their applications, only two departments responded.

Risk: With city departments failing to participate in disaster recovery testing, there is a risk that the disaster recovery plan may not work as anticipated, which could potentially reduce OIT's ability to restore services in a timely fashion.

Recommendation: We recommend that OIT revise the disaster recovery plan to require city departments' involvement as a success factor for the test plan [300416.10].

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 general IT controls. While several previously reported issues remained uncorrected and were discussed in the preceding section of this report,[4] our testing found that the following prior-noted conditions were resolved:

Organizational and Management Controls

Vendor Management

Condition: Reports on the internal control environments at third-party service providers (in accordance with Statement on Standards for Attestation Engagements (SSAE) 16) were not consistently obtained and reviewed by OIT [300413.02].

[4] The uncorrected prior year issues involved the OIT's failure to perform a comprehensive IT risk assessment; change management procedures not being consistently followed; certain OIT programmers' having the ability to change payroll data; password configurations not always being consistently implemented or in compliance with established policies; the lack of business continuity plans for city systems; and the failure to test the Basis2 disaster recovery plan.

Remediation Status: **Complete –** During the current review, we observed that there was a vendor management process in place for contract monitoring. Also, we noted that none of the in-scope applications were hosted offsite which would result in the need for a SSAE 16 report.

IT Policies and Procedures

Condition: OIT did not consistently document the review and approval of governing IT policies and procedures [300413.03].

Remediation Status: **Complete –** In the prior review, OIT had provided a draft policy setting forth a standard process for the development, review, and approval of its operating policies and procedures; however, the policy was still awaiting final approval. During our current review, we noted that the policy was signed off by OIT executive management.

Technical Infrastructure

Domain Administrators

Condition: An excessive number of accounts were included in the membership of the domain administrators group within the Active Directory. Also, the active domain administrators list contained several service accounts with generic user names [300413.04].

Remediation Status: **Complete** – Our current review found that OIT's executive management approved a formal policy which requires an annual review of domain administrator access for appropriateness. We observed the annual review and noted that each domain administrator account was reviewed and approved. Additionally, our testing found that all domain administrator accounts were appropriate, including the service accounts which were associated with specific individuals or service organizations.

Data Administration

Basis2 Backup Media

Condition: Media used to store backups of the Basis2 application were not stored off-site [300413.06].

Remediation Status: **Complete –** During the previous review, OIT management informed the Controller's Office that they had ordered the equipment needed to add Basis2 to the backup tape library process, and the equipment was due for installation and testing by January 2016. Our current testing noted that OIT completed the installation of this equipment.

Application Administration

Vendor Support Access

Condition: Vendor support accounts were provided full access to Basis2 and were active [300413.08].

Remediation Status: **Complete** – Our current testing noted that (1) OIT implemented a monitoring process for vendor support accounts and (2) vendor support accounts had end dates to their access rights.

IT Operations and Support

Programmer Access Rights

Condition: Several consultants from a firm that provided programming services also had the ability to add, modify, and delete TIPS transaction data [500114.13].

Remediation Status: **Complete** – The current review found that the programming consultants' access had been appropriately restricted.

Termination of TIPS User IDs

Condition: Access of separated employees to the TIPS application was not always disabled and removed in a timely manner [500114.14].

Remediation Status: **Complete** – During the current review, we noted that OIT generated bi-weekly listings of terminated users for research and removal of access, and contractors were monitored on a thirty day basis. Also, our testing noted no issues related to the disabling of accounts for separated employees.

Software Administration

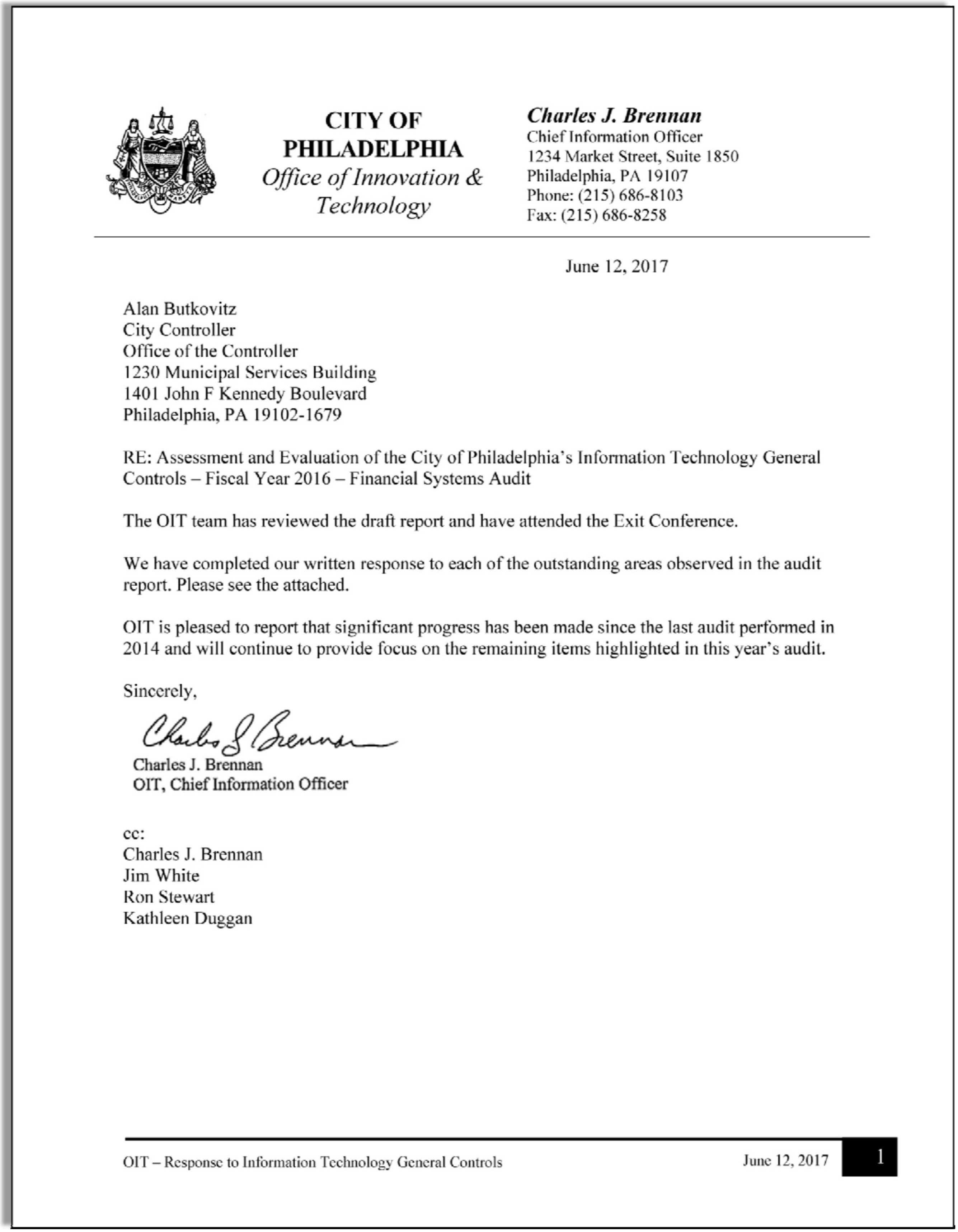
Application Change Management

Condition: While the Revenue IT group had developed a change management policy for TIPS, the policy lacked sufficient details on certain steps in the change management process, such as standard criteria for user testing of application changes and documentation requirements for the user's approval of the change [500114.15].

Remediation Status: **Complete** – The current review disclosed that the TIPS change management policy was updated to include reference to end user testing and approval requirements.

SECTION II

MANAGEMENT’S RESPONSE



CITY OF PHILADELPHIA
Office of Innovation & Technology

Charles J. Brennan
Chief Information Officer
1234 Market Street, Suite 1850
Philadelphia, PA 19107
Phone: (215) 686-8103
Fax: (215) 686-8258

June 12, 2017

Alan Butkovitz
City Controller
Office of the Controller
1230 Municipal Services Building
1401 John F Kennedy Boulevard
Philadelphia, PA 19102-1679

RE: Assessment and Evaluation of the City of Philadelphia's Information Technology General Controls – Fiscal Year 2016 – Financial Systems Audit

The OIT team has reviewed the draft report and have attended the Exit Conference.

We have completed our written response to each of the outstanding areas observed in the audit report. Please see the attached.

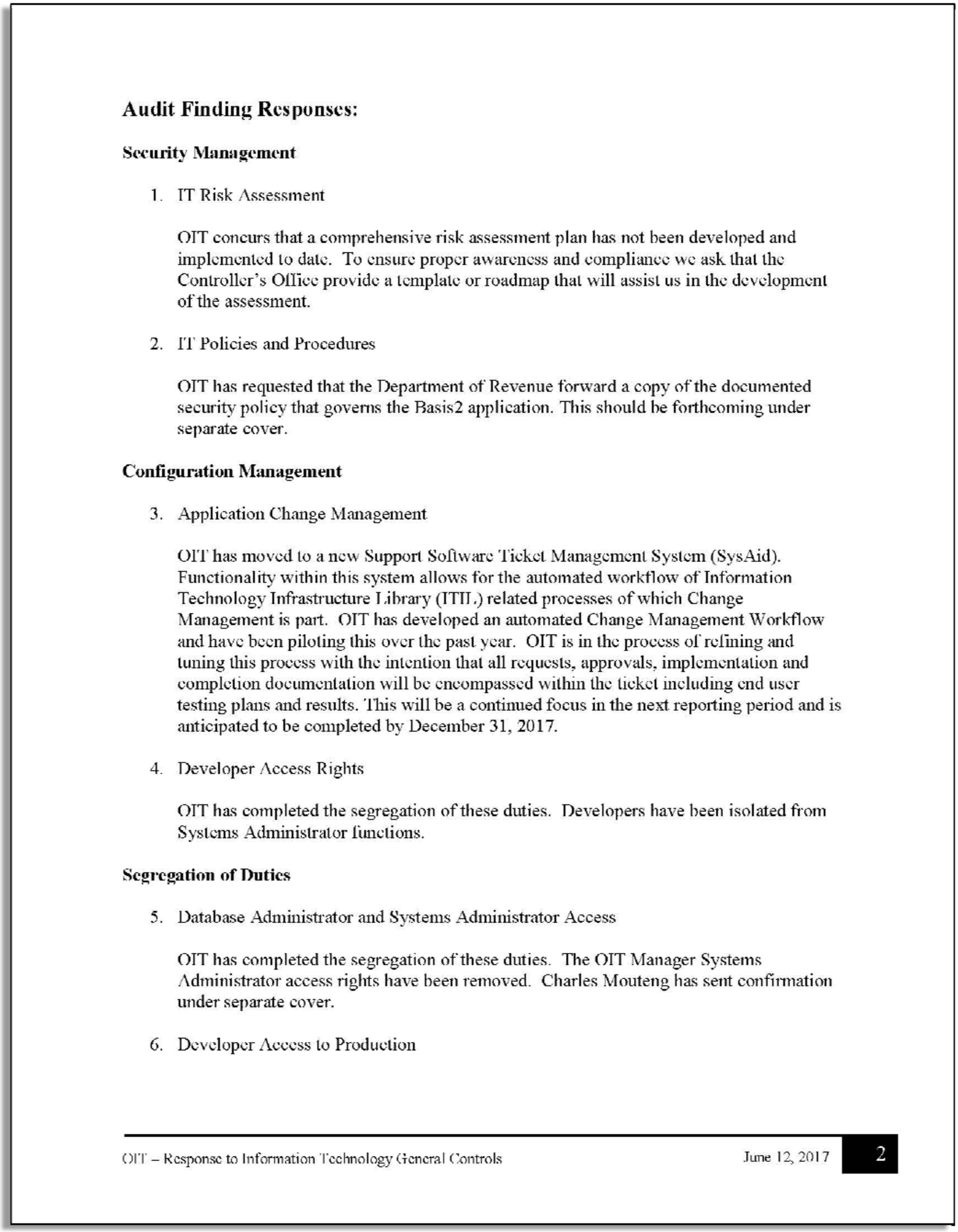
OIT is pleased to report that significant progress has been made since the last audit performed in 2014 and will continue to provide focus on the remaining items highlighted in this year's audit.

Sincerely,

Charles J Brennan

Charles J. Brennan
OIT, Chief Information Officer

cc:
Charles J. Brennan
Jim White
Ron Stewart
Kathleen Duggan



Audit Finding Responses:

Security Management

1. IT Risk Assessment

   OIT concurs that a comprehensive risk assessment plan has not been developed and implemented to date. To ensure proper awareness and compliance we ask that the Controller's Office provide a template or roadmap that will assist us in the development of the assessment.

2. IT Policies and Procedures

   OIT has requested that the Department of Revenue forward a copy of the documented security policy that governs the Basis2 application. This should be forthcoming under separate cover.

Configuration Management

3. Application Change Management

   OIT has moved to a new Support Software Ticket Management System (SysAid). Functionality within this system allows for the automated workflow of Information Technology Infrastructure Library (ITIL) related processes of which Change Management is part. OIT has developed an automated Change Management Workflow and have been piloting this over the past year. OIT is in the process of refining and tuning this process with the intention that all requests, approvals, implementation and completion documentation will be encompassed within the ticket including end user testing plans and results. This will be a continued focus in the next reporting period and is anticipated to be completed by December 31, 2017.

4. Developer Access Rights

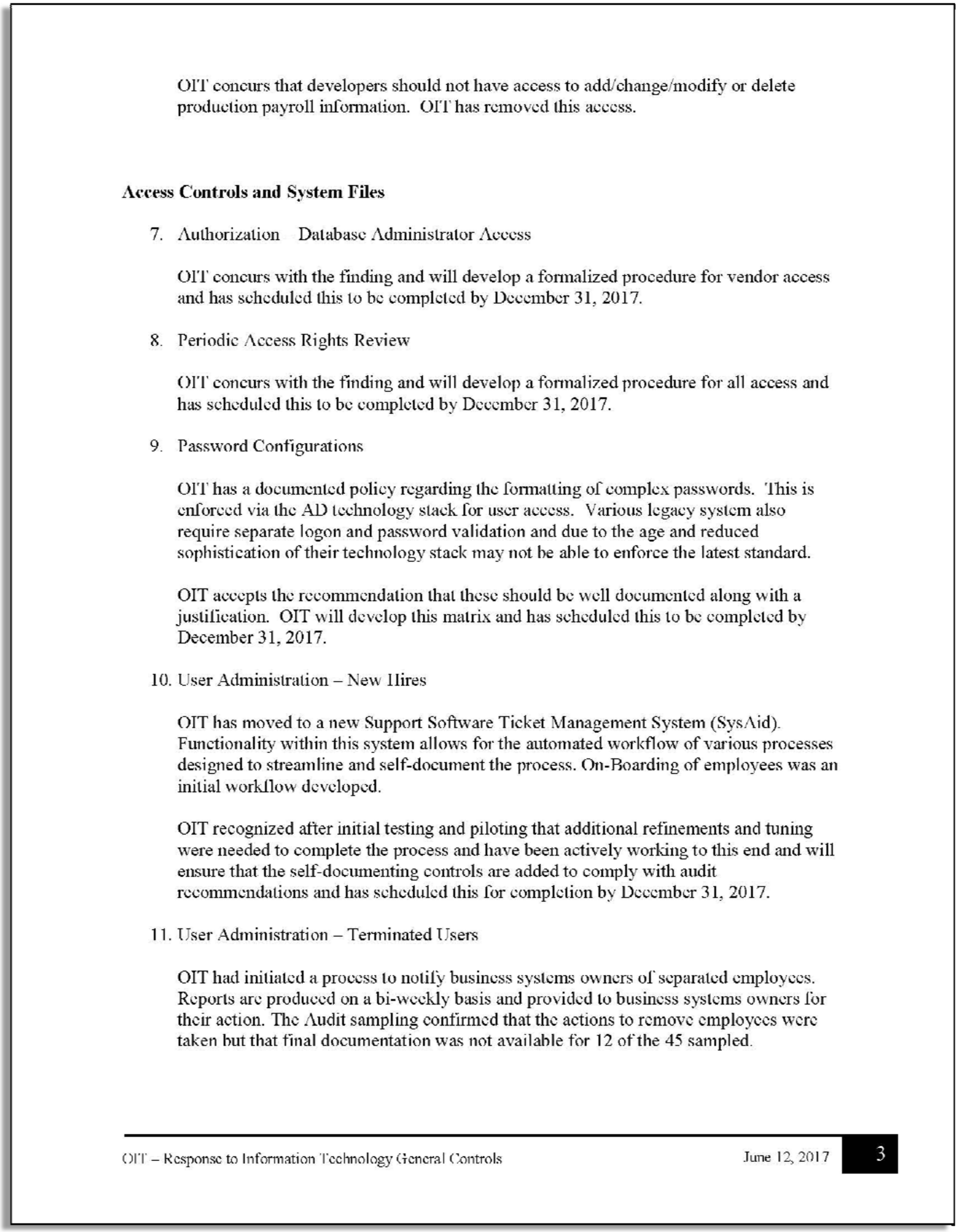
   OIT has completed the segregation of these duties. Developers have been isolated from Systems Administrator functions.

Segregation of Duties

5. Database Administrator and Systems Administrator Access

   OIT has completed the segregation of these duties. The OIT Manager Systems Administrator access rights have been removed. Charles Mouteng has sent confirmation under separate cover.

6. Developer Access to Production



OIT concurs that developers should not have access to add/change/modify or delete production payroll information. OIT has removed this access.

Access Controls and System Files

7. Authorization Database Administrator Access

   OIT concurs with the finding and will develop a formalized procedure for vendor access and has scheduled this to be completed by December 31, 2017.

8. Periodic Access Rights Review

   OIT concurs with the finding and will develop a formalized procedure for all access and has scheduled this to be completed by December 31, 2017.

9. Password Configurations

   OIT has a documented policy regarding the formatting of complex passwords. This is enforced via the AD technology stack for user access. Various legacy system also require separate logon and password validation and due to the age and reduced sophistication of their technology stack may not be able to enforce the latest standard.

   OIT accepts the recommendation that these should be well documented along with a justification. OIT will develop this matrix and has scheduled this to be completed by December 31, 2017.

10. User Administration – New Hires

    OIT has moved to a new Support Software Ticket Management System (SysAid). Functionality within this system allows for the automated workflow of various processes designed to streamline and self-document the process. On-Boarding of employees was an initial workflow developed.

    OIT recognized after initial testing and piloting that additional refinements and tuning were needed to complete the process and have been actively working to this end and will ensure that the self-documenting controls are added to comply with audit recommendations and has scheduled this for completion by December 31, 2017.

11. User Administration – Terminated Users

    OIT had initiated a process to notify business systems owners of separated employees. Reports are produced on a bi-weekly basis and provided to business systems owners for their action. The Audit sampling confirmed that the actions to remove employees were taken but that final documentation was not available for 12 of the 45 sampled.

OIT agrees with the audit recommendation that this process should be expanded to include formal review, notification and documentation of the completed actions. OIT will define a process by December 31, 2017 and will subsequently schedule an implementation process before the next reporting cycle of June 30, 2018.

12. User Administration – Notification of Terminated and Inactive Users

    Similar to point // 11 above, OIT will define a process by December 31, 2017 and will subsequently schedule an implementation process before the next reporting cycle of June 30, 2018 to provide notification to Payroll, Pension Payroll and Health and Welfare application groups.

13. Wireless Network

    Remediated prior to exit conference, finding closed.

Contingency Planning

14. Business Continuity Plan

    The Office of Emergency Management oversees Department Business Continuity planning efforts. We will past this recommendation on to that Office.

15. Basis2 Disaster Recovery

    OIT recognizes the need for Disaster Recovery and that reasonable on-site redundancy is built into the current support model. However offsite disaster recovery is not available at the present time. OIT is actively working towards a longer-range DR offering leveraging alternate offsite resources. Basis2 will be a high priority item for off-site DR.

16. Disaster Recovery Testing

    OIT performs a semi-annual offsite DR test for its mainframe platform. OIT did note that end user business owner participation was lower during the last test than in previous tests. OIT agrees with the audit finding and has already contacted business users to re-iterate the need for their future participation. OIT will escalate the need to upper management as appropriate to ensure participation in the next semi-annual test scheduled for June 22, 2017.