CITY OF PHILADELPHIA
PENNSYLVANIA

OFFICE OF THE CONTROLLER

Promoting honest, efficient, and fully accountable government

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

FISCAL 2013

City Controller
ALAN BUTKOVITZ

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

GERALD V. MICCIULLA
Deputy City Controller

November 25, 2013

Adel Ebeid
Chief Innovation Officer
Office of Innovation and Technology
1234 Market Street, 18th Floor
Philadelphia, PA 19107

Dear Mr. Ebeid:

The Office of the Controller commissioned and oversaw an assessment, conducted by the independent accounting firm of CliftonLarsonAllen 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, 2013. 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 you and 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 Michael A. Nutter, Mayor
Honorable Darrell L. Clarke, President
And Honorable Members of City Council
Members of the Mayor's Cabinet
Rob Dubow, Director of Finance

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 CliftonLarsonAllen, LLP., to conduct an assessment of the Information Technology (IT) general controls implemented by the Office of Innovation & 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, 2013.

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.

- A comprehensive IT risk assessment, to identify and track operational and compliance risks, was not performed by OIT. This situation increases the risk that limited IT resources are not effectively or efficiently deployed in supporting city operations.
- Procedures requiring approval and documentation of changes to the IT system 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 system.
- A formalized business continuity plan had not been developed. In the event of a disruption to city IT systems, departments and agencies may not be able to provide required services or continue operations until service is restored.
- System access rights of inactive or terminated employees or contractors were not periodically reviewed for removal. Access of sensitive information by unauthorized users could compromise security.
- A disaster recovery plan and subsequent testing of the plan had not been formally documented or performed for the city's BASIS2 water billing system. In addition, backups of BASIS2 were not stored off-site. In the event of a disaster, the recovery plan may not work as anticipated and backups of system data may not be available.

What the Controller's Office Recommends

The city's Office of Innovation and Technology should (1) develop formal procedures to perform periodic risk assessments and monitor identified gaps; (2) strengthen change management procedures and ensure that required documentation and approvals are obtained; (3) assist city departments and agencies in establishing business continuity plans; 4) implement procedures to remove or disable employee access immediately upon termination; and 5) develop, document and periodically test a disaster recovery plan for BASIS2. These and other proposed actions are more fully described in the body of the report.

Section

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

CliftonLarsonAllen LLP
CLAconnect.com

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, 2013. 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 July through September 2013.

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.

CliftonLarsonAllen LLP

CliftonLarsonAllen LLP

Plymouth Meeting, Pennsylvania
October 2, 2013

City of Philadelphia – Office of the City Controller
Assessment and Evaluation of the Office of Innovation and Technology of Philadelphia's IT General Controls
As of June 30, 2013

Table of Contents

City of Philadelphia – Office of the City Controller
Assessment and Evaluation of the Office of Innovation and Technology of Philadelphia's IT General Controls
As of June 30, 2013

Executive Summary

The City Controller's Office engaged CliftonLarsonAllen (CLA) to perform an assessment of Information Technology (IT) general controls related to the City of Philadelphia's Office of Innovation and Technology's (OIT) 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, 2013.

Summary of Objective, Scope and Methodology

The objective of the CLA consulting engagement was to provide an assessment and evaluation of the Information Technology (IT) general controls implemented by the City of Philadelphia's Office of Innovation and Technology (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, 2013. Our engagement was structured to address the following eight (8) domains as requested by the City Controller's Office:

Organization and Management Controls	Application Administration
Technical Infrastructure	IT Operations & Support
Software Administration	Physical Environment
Data Administration	Business Continuity

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

- Financial Accounting Management Information System (FAMIS)
- Payroll
- Pension Payroll
- Taxpayer Inquiry and Payment System (TIPS)
- Health and Welfare
- Basis2

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, 2013

Summary of Observations
Below we are providing a summary of our key observations noted through the procedures performed for this engagement that could have a high or moderate impact on the operations and internal controls of OIT. Additional details for these observations as well as other observations with low impact are provided in the detailed section of our report.

Domain	Findings	Potential Impact
Organization and Management Controls	1. **Comprehensive Risk Assessment** – A formalized risk assessment is not periodically performed. 2. **Vendor Management** – Third-party control reports are not obtained and reviewed.	High Moderate
Technical Infrastructure	3. **Domain Administrators** – Excessive number of accounts were granted membership to the Domain Administrator Group.	Moderate
Software Administration	4. **Change Management** – Change management procedures are not consistently followed.	High
Data Administration	5. **BASIS2 Media Backup** – Copies of backup media are not stored off-site	Moderate
Application Administration	6. **Periodic Access Rights Review** – A process has not been implemented to review active application accounts and related access permissions periodically. 7. **Vendor Support Accounts** – BASIS2 vendor support accounts are granted full access to the system and are not de-activated when not in use.	Moderate Moderate
IT Operations & Support	8. **Termination of Payroll and FAMIS IDs** – Accounts of terminated employees were noted with access to Payroll and FAMIS applications.	Moderate
Physical Environment	None noted.	
Business Continuity	9. **Business Continuity Plan** – A formalized business continuity plan has not been developed. 10. **BASIS2 Disaster Recovery** – A disaster recovery plan has not been formally documented or tested for the BASIS2 application.	Moderate Moderate

Detailed Results

Objective, Scope and Methodology

The objective of the CLA consulting engagement was to provide an assessment and evaluation of the Information Technology (IT) general controls implemented by the OIT in support of the City Controller's Office audit of the Comprehensive Annual Financial Report (CAFR) of the City. Our engagement was structured to address the eight (8) domains as outlined in our proposal. Within each domain we focused on several control elements as follows:

Domain	Focus
Organization and Management Controls	• IT Organization & Governance • Policies, Standards & Guidelines • Personnel Administration • Vendor Administration • Technology Administration
Technical Infrastructure	• Technical Documentation & Illustration(s) • Network Administration • Server Administration • Workstation Administration • Peripheral Administration
Software Administration	• Software Asset Administration • Software Development Administration • Software Change Management
Data Administration	• Data Management • Database Administration (*If Applicable*) • Data Transfer(s) Administration • Data Storage & Backup Administration
Application Administration	• Access Controls & Permissions • Business Rules/Parameters • Data Input/Processing/Output • Data Maintenance • Activity Logging/Monitoring
IT Operations & Support	• User Account Administration • IT Systems Operations • Problem Management (*Help Desk*)
Physical Environment	• Physical Security • Environment Controls
Business Continuity	• Incident Response • Disaster Recovery

Background Information on Office of Innovation and Technology System and Administering Personnel

The Office of Innovation and Technology's (OIT) mission is to increase the effectiveness of the information technology infrastructure, where the services are advanced, optimized, and responsive to the needs of the City of Philadelphia's businesses, residents and visitors.

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.

To this end, OIT provides the following services:

Business Improvement Services
Business Improvement Services (BIS) primary objective is to work with business partners in the City's Agencies and Departments to maximize the benefits of these initiatives. This starts with clearly defining the needs — not just technology solutions and application systems but the process improvements, metrics of performance, informational needs and organizational change. BIS is responsible for ensuring the scoping, planning, resourcing and effective execution from concept through completion of these initiatives. Key service offerings include: Business Analysis; Program and Project Management; Systems Planning; Software Selection; Enabling Technologies.

Applications and Information Services
Application and Information Services primarily is responsible for continuing development and maintenance of core applications, department applications, and information management citywide. OIT provides oversight and direction for the applications and tools used throughout the City to deliver Internet/Intranet services to City employees and the public. Key service offerings include: Software Development; Application Maintenance and Support; Information Management Support; Quality Assurance; Philadelphia Web Applications; GIS. The following applications were included in our scope:

- Financial Accounting Management Information System (FAMIS)
- Payroll
- Pension Payroll
- Taxpayer Inquiry and Payment System (TIPS)
- Health and Welfare
- Basis2

Operations and Communication Services
Key service offerings include: Communications; Radios; Video Surveillance; 911 Support; Production Operations; Cable Franchise.

Infrastructure Services
Infrastructure services manages and ensures the security and safety of the City's computing operations including supporting the infrastructure necessary to deploy, operate, and maintain the city's communications and information systems. Key service offerings include: PC Support; Helpdesk; Network Management; Server Management; Data Center Management; Messaging; Information Security.

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.

Organizational and Management Controls

1. IT Risk Assessment

   Condition: A comprehensive IT risk assessment has not been performed. While the Office of Information Technology (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.

   Potential Impact: **High**

2. Vendor Management

   Condition: Reports on the internal controls environments at third-party service providers are not consistently obtained and reviewed. OIT had not obtained and reviewed the Statement on Standards for Attestation Engagements (SSAE) 16 Report for Official Payments, credit card processor. This report excluded the primary business operations provided to the City. These reports allow the City to monitor the effectiveness of the controls environments in situations where financial transactions are processed on behalf of the City.

   Risk: A lack of documented due diligence procedures by the City over the reliance on service providers could lead to critical risk being inadvertently inherited by the City.

   Recommendation: We recommend that the City develop a process to periodically assess the internal controls environment at third-party service providers. And coordinate with vendors, such as Official Payments, to obtain more structured and detailed internal control reports.

   Potential Impact: **Moderate**

3. IT Policies and Procedures

   Condition: OIT does not consistently document the review and approval of governing IT policies and procedures.

   Risk: Lack of clarity for OIT personnel on operating policies and procedures increases the risk that policies and procedures do not reflect current operating procedures.

Recommendation: We recommend that OIT develop processes to periodically review, update, and approve operating policies and procedures and that such reviews be documented.

Potential Impact: ***Low***

Technical Infrastructure

4. Domain Administrators

Condition: An excessive number of accounts were included in the membership of the domain administrators group within Active Directory.

Risk: Excessive domain administrators increases the risk that unauthorized or undetected changes to settings or data will occur.

Recommendation: We recommend that OIT review the current listing of domain administrators and restrict access where appropriate. Additionally procedures should be developed to periodically review administrator access for appropriateness.

Potential Impact: **Moderate**

Software Administration

5. Application Change Management

Condition: While OIT has developed a change management procedure, the procedure is inconsistently applied when performing change requests for in scope applications. 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.

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 its procedures and implement steps to ensure that required documentation and steps are performed and documented.

Potential Impact: **High**

Data Administration

6. BASIS2 Backup Media

Condition: Media used to store backups of the BASIS2 application are not stored off-site.

Risk: In the event of a disaster, backup media may not be available.

Recommendation: We recommend that OIT evaluate separate locations to store rotated backup media.

Potential Impact: **Moderate**

Application Administration

7. Periodic Access Rights Review

Condition: A process has not been implemented to periodically review active application user accounts, associated access rights, and group membership.

Risk: While OIT has implemented processes to perform and approve granting of user access, changes to user access, and removal of access rights, 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, develop a procedure to periodically review the active users and their associate access rights for appropriateness.

Potential Impact: **Moderate**

8. Vendor Support Access

Condition: Vendor support accounts are provided full access to BASIS2 and are active.

Risk: Increases the risk that unauthorized transactions or activities will be performed without the City's knowledge.

Recommendation: We recommend that vendor support accounts only be granted access they need to provide ongoing support and that a process be implemented to activate support accounts when vendor is providing support.

Potential Impact: ***Moderate***

9. Password Configurations

Condition: 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:

- Network:
  - Minimum Password Length set to 7 characters
  - Account Lockout Duration set to 15 minutes
- RACF
  - Minimum Password Age is disabled
- Natural
  - Password History has not been enabled
  - Password Complexity has not been enabled
- Oracle Database
  - Configurations have not been established

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.

Potential Impact: **Low**

IT Operations & Support

10. Privileged RACF Access

Condition: RACF privileged accounts with the SPECIAL and OPERATOR attributes have not been segregated from those with the AUDITOR attribute. The SPECIAL attribute allows users to perform system administrator functions, including adding and removing users, granting access to datasets and resources and setting RACF configuration settings. The OPERATOR attribute permits users to alter any dataset that they are not specifically restricted from in the dataset access rule. The AUDITOR attribute allows users to control the logging functionality of RACF.

Risk: Privileged users would be able to remove logging requirements from RACF and enhance their ability to perform unauthorized activity undetected.

Recommendation: Upon our recommendation, OIT has removed the AUDITOR attribute from identified accounts.

Potential Impact: **Low**

11. IBMUSER Account

Condition: The default RACF account, IBMUSER, is not revoked when use is not required.

Risk: Compromise of the IBMUSER account would provide full access to the RACF environment.

Recommendation: Upon our recommendation, OIT has revoked the account and will implement procedures to maintain the account as needed.

Potential Impact: **Low**

12. Termination of Payroll and FAMIS IDs

Condition: Payroll and FAMIS accounts for terminated employees were not removed or disabled in a timely manner.

Risk: User may be able to access system resources after employment with the City has been terminated.

Recommendation: We recommend that OIT review its procedures to identify and take action on terminated employees.

Potential Impact: **Moderate**

Physical Environment

No relevant findings noted as a result of our procedures for this domain.

Business Continuity

13. Business Continuity Plan

Condition: A business continuity plan has not 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.

Potential Impact: **Moderate**

14. BASIS2 Disaster Recovery

Condition: The disaster recovery plan and subsequent testing of the plan have not been formally documented or performed.

Risk: The recovery plan may not be available or known to key individuals or may not work as anticipated when faced with an unplanned outage.

Recommendation: We recommend that OIT develop, document, and periodically test a disaster recovery plan for the BASIS2 application and infrastructure.

Potential Impact: **Moderate**

15. Disaster Recovery Plan

Condition: The disaster recovery plan established for the mainframe applications did not include all pertinent information needed to perform the restoration activities, including:

- Location of the off-site facility
- Instruction to retrieve back-up media

Risk: Lack of such plan details could potentially reduce OIT's ability to restore services in a timely fashion.

Recommendation: We recommend that OIT include the noted items in the disaster recovery plan.

Potential Impact: **Low**

SECTION II

MANAGEMENT'S RESPONSE

CITY OF PHILADELPHIA
Office of Innovation & Technology

Adel W. Ebeid
Chief Innovation Officer
1234 Market Street, Suite 1850
PHILADELPHIA, PA 19102-3721
Phone: (215) 686 – 8103
FAX: (215) 686 – 8258

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 2013

The OIT team has reviewed the draft report and is prepared for the planned discussion.

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

Sincerely,

By- Jim White OIT-COO
For - Adel Ebeid

OIT, Chief Innovation Officer

cc:

Adel Ebeid
Jim White
Ron Stewart
Gloria Mitchell-Piper

ASSESSMENT AND EVALUATION
CITY OF PHILADELPHIA
INFORMATION TECHNOLOGY GENERAL CONTROLS – FINANCIAL SYSTEMS AUDIT

Original Assessment (6.30.2013)

REPORT NO. 2013-1030 **REVISED 11/6/2013**

Finding No(s).	Program /Area	Recommendation	Status	Comments
No. 1	Organization and Management Controls	IT Risk Assessment: 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.	Pending	OIT is aware that a holistic risk assessment program should be developed and periodically performed to assess the impact on the organization. Initial discussions have been held to lay the framework for such a program.
No. 2		Vendor Management: We recommend that the City develop a process to periodically assess the internal controls environment at third-party service providers.	In-Progress	OIT concurs with this recommendation and will develop processes to assess the internal controls of its third party providers.
No. 3		IT Policies and Procedures: We recommend that OIT develop processes to periodically review and approve operating policies and procedures and that such reviews be documented.	In-Progress	OIT is currently documenting a standard policy and procedure for the development and maintenance of policies and procedures which includes a periodic annual review of all policies and procedures..
No. 4	Technical Infrastructure	Domain Administrators: We recommend that OIT review the current listing of domain administrators and restrict access where appropriate. Additionally procedures should be developed to periodically review administrator access for appropriateness.	In-Progress	A review has been initiated to address the current finding identified and a policy and procedure will be developed to formalize the process.
No. 5	Software Administration	Application Change Management: We recommend that OIT review its procedures and implement steps to ensure that required documentation and steps are performed and documented.	In-Progress	OIT is currently revising its change management process in conjunction with adopting ITIL best practices. Application change will be reviewed and where appropriate ensure proper documentation is provided to support all application changes.
No. 6	Data Administration	BASIS2 Backup Media: We recommend that OIT evaluate separate locations to store rotated backup media.	In-Progress	We concur with this recommendation and will implement offsite rotation of backups..
No.7	Application Administration	Periodic Access Rights Review: We recommend that OIT, along with impacted departments, develop a procedure to periodically review the active users and their associate access rights for appropriateness.	In-Progress	OIT has initiated phase one of this review at a macro level in that we periodically review all severed employees for removal from access lists. OIT will work with business owners to develop processes for periodic validation of users access.
No.8		Vendor Support Access: We recommend that vendor support accounts only be granted access they need to provide ongoing support and that a process be implemented to activate support accounts when vendor is providing support.	In-Progress	OIT is reviewing the current internal controls around granting vendor access and related rights.
No.9		Password Configurations: We recommend that OIT review the available configurations of each authentication point and evaluate strengthening the configuration.	In-Progress	OIT Security Office will review the current operational protocols for consistency with established standards and initiate changes where necessary working with the business owners.
No.10		Privileged RACF Access – remove Auditor attribute from identified accounts.	Competed	OIT has removed the AUDITOR attribute from identified accounts.

ASSESSMENT AND EVALUATION
CITY OF PHILADELPHIA
INFORMATION TECHNOLOGY GENERAL CONTROLS – FINANCIAL SYSTEMS AUDIT

Original Assessment (6.30.2013)

REPORT NO. 2013-1030 **REVISED 11/6/2013**

Finding No(s).	Program /Area	Recommendation	Status	Comments
No.11		IBMUSER Account: revoked the account and l implement procedures to maintain the account as needed.	Completed	OIT has revoked the account and will implement procedures to maintain the account as needed.
No.12		Termination of Payroll and FAMIS IDs: We recommend that OIT review its procedures to identify and take action on terminated employees.	In-Progress	A process has been initiated to produce a list of inactive employees which will be used to drive the access rights changes. Processes need to be refined to institutionalize these changes.
No.13	Business Continuity	Business Continuity Plan: We recommend that OIT communicate with potential 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.	In-Progress	OIT understands that business continuity planning is a departmental responsibility and recognizes that it is a key component to supporting this planning process. We plan on working closely with departments in the development of their plans where there is an intersection of business and technology.
No.14		BASIS2 Disaster Recovery: We recommend that OIT develop, document, and periodically test a disaster recovery plan for the BASIS2 application and infrastructure.	Pending	Disaster Recovery has been identified as a need in our capital planning budgetary process and a line item has been added to provide planning resources.
No.15		Disaster Recovery Plan: We recommend that OIT include the noted items in the disaster recovery plan. • Location of the off-site facility • Instruction to retrieve back-up media	Pending	See note 14