

**GOVERNMENT OF THE DISTRICT OF COLUMBIA
OFFICE OF THE INSPECTOR GENERAL**

**UNIVERSITY OF THE
DISTRICT OF COLUMBIA**

**Report on Internal Control and Compliance
Over Financial Reporting
for the Year Ended
September 30, 2012**



**CHARLES J. WILLOUGHBY
INSPECTOR GENERAL**

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Office of the Inspector General

Inspector General



May 31, 2013

The Honorable Vincent C. Gray
Mayor
District of Columbia
Mayor's Correspondence Unit, Suite 316
1350 Pennsylvania Avenue, N.W.
Washington, D.C. 20004

The Honorable Phil Mendelson
Chairman
Council of the District of Columbia
John A. Wilson Building, Suite 504
1350 Pennsylvania Avenue, N.W.
Washington, D.C. 20004

Dear Mayor Gray and Chairman Mendelson:

In connection with the audit of the District of Columbia's (the District) general purpose financial statements for fiscal year (FY) 2012, KPMG LLP (KPMG) submitted the enclosed report on internal control and on compliance and other matters for the University of the District of Columbia (UDC) for FY 2012 (OIG No. 13-1-07GG(a)). This report sets forth KPMG's comments and recommendations to improve internal control and other operating efficiencies.

The report identifies three deficiencies – one a material weakness and other deficiencies considered to be significant deficiencies. A deficiency in internal control over financial reporting exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A material weakness is a deficiency, or combination of deficiencies, in internal control over financial reporting, 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. KPMG considers UDC's Lack of Controls Over the Implementation of the Banner System, which is described in item 2012-01, to be a material weakness.

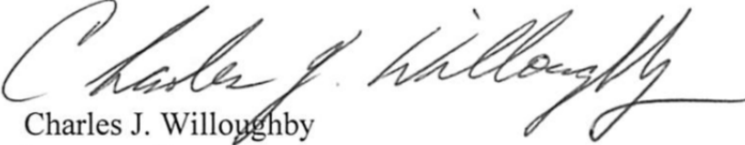
A significant deficiency is a deficiency, or a combination of deficiencies, in internal control over financial reporting that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. The two significant deficiencies identified in the report are as follows: Lack of Controls Over the Financial Reporting Process (2012-02); and Lack of Controls Over Compliance With Investment Policy (2012-03).

Mayor Gray and Chairman Mendelson
Report on Internal Control and on Compliance and Other
Matters for UDC
OIG No. 13-1-07GG(a) – Final Report
May 31, 2013
Page 2 of 4

The results of tests performed by KPMG disclosed no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards*.

If you have questions or need additional information, please contact Ronald W. King, Assistant Inspector General for Audits, at (202) 727-2540.

Sincerely,



Charles J. Willoughby
Inspector General

CJW/ws

Enclosure

cc: See Distribution List

DISTRIBUTION:

Mr. Allen Y. Lew, City Administrator, District of Columbia (via email)
Mr. Victor L. Hoskins, Deputy Mayor for Planning and Economic Development, District of Columbia (via email)
The Honorable Kenyan McDuffie, Chairperson, Committee on Government Operations, Council of the District of Columbia (via email)
The Honorable Yvette Alexander, Chairperson, Committee on Health, Council of the District of Columbia (via email)
Mr. Brian Flowers, General Counsel to the Mayor (via email)
Mr. Christopher Murphy, Chief of Staff, Office of the Mayor (via email)
Ms. Janene Jackson, Director, Office of Policy and Legislative Affairs (via email)
Mr. Pedro Ribeiro, Director, Office of Communications, (via email)
Mr. Eric Goulet, Budget Director, Mayor's Office of Budget and Finance (1 copy)
Ms. Nyasha Smith, Secretary to the Council (1 copy and via email)
Mr. Irvin B. Nathan, Attorney General for the District of Columbia (via email)
Dr. Natwar M. Gandhi, Chief Financial Officer (1 copy and via email)
Mr. Mohamad Yusuff, Interim Executive Director, Office of Integrity and Oversight, Office of the Chief Financial Officer (via email)
Ms. Yolanda Branche, D.C. Auditor (1 copy)
Mr. Phillip Lattimore, Director and Chief Risk Officer, Office of Risk Management (via email)
Mr. Steve Sebastian, Managing Director, FMA, GAO, (via email)
The Honorable Eleanor Holmes Norton, D.C. Delegate, House of Representatives, Attention: Bradley Truding (via email)
The Honorable Darrell Issa, Chairman, House Committee on Oversight and Government Reform, Attention: Howie Denis (via email)
The Honorable Elijah Cummings, Ranking Member, House Committee on Oversight and Government Reform, Attention: Yvette Cravins (via email)
The Honorable Thomas Carper, Chairman, Senate Committee on Homeland Security and Governmental Affairs, Attention: Holly Idelson (via email)
The Honorable Tom Coburn, Ranking Member, Senate Committee on Homeland Security and Governmental Affairs, Attention: Katie Bailey (via email)
The Honorable Mark Begich, Chairman, Senate Subcommittee on Emergency Management, Intergovernmental Relations and the District of Columbia, Attention: Cory Turner (via email)
The Honorable Rand Paul, Ranking Member, Senate Subcommittee on Emergency Management, Intergovernmental Relations and the District of Columbia (1 copy)
The Honorable Harold Rogers, Chairman, House Committee on Appropriations, Attention: Amy Cushing (via email)
The Honorable Nita Lowey, Ranking Member, House Committee on Appropriations, Attention: Laura Hogshead (via email)
The Honorable Ander Crenshaw, Chairman, House Subcommittee on Financial Services and General Government, Attention: Amy Cushing (via email)
The Honorable José E. Serrano, Ranking Member, House Subcommittee on Financial Services and General Government, Attention: Laura Hogshead (via email)

Mayor Gray and Chairman Mendelson
Report on Internal Control and on Compliance and Other
Matters for UDC
OIG No. 13-1-07GG(a) – Final Report
May 31, 2013
Page 4 of 4

The Honorable Barbara Mikulski, Chairwoman, Senate Committee on Appropriations,
Attention: Ericka Rojas (via email)
The Honorable Richard Shelby, Ranking Member, Senate Committee on Appropriations,
Attention: Dana Wade (via email)
The Honorable Frank Lautenberg, Chairman, Senate Subcommittee on Financial Services
and General Government, Attention: Marianne Upton (via email)
The Honorable Mike Johanns, Ranking Member, Senate Subcommittee on Financial Services
and General Government, Attention: Dale Cabaniss (via email)
Mr. Paul Geraty, CPA, Public Sector Audit Division KPMG LLP (1 copy)



KPMG LLP
Suite 12000
1801 K Street, NW
Washington, DC 20006

Independent Auditors' Report on Internal Control over Financial Reporting and on Compliance and Other Matters Based on an Audit of Financial Statements Performed in Accordance with *Government Auditing Standards*

The Board of Trustees
University of the District of Columbia
Washington, District of Columbia:

We have audited the basic financial statements of the University of the District of Columbia (the University), a component unit of the Government of the District of Columbia, as of and for the year ended September 30, 2012, and have issued our report thereon dated January 31, 2013. We conducted our audit in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States.

Internal Control over Financial Reporting

Management of the University is responsible for establishing and maintaining effective internal control over financial reporting. In planning and performing our audit, we considered the University's internal control over financial reporting as a basis for designing our auditing procedures for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the University's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of the University's internal control over financial reporting.

Our consideration of internal control over financial reporting was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control over financial reporting that might be significant deficiencies or material weaknesses and therefore, there can be no assurance that all deficiencies, significant deficiencies, or material weaknesses have been identified. However, as discussed below, we identified certain deficiencies in internal control over financial reporting that we consider to be a material weakness and other deficiencies that we consider to be significant deficiencies.

A deficiency in internal control over financial reporting exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A material weakness is a deficiency, or combination of deficiencies, in internal control over financial reporting, 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. We consider the deficiency in the University's internal control over financial reporting, which is described in the accompanying schedule of findings and responses as item 2012-01 to be a material weakness.

A significant deficiency is a deficiency, or combination of deficiencies, in internal control over financial reporting that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. We consider the deficiencies, which are described in the accompanying schedule of findings and responses as items 2012-02 and 2012-03 to be significant deficiencies in internal control over financial reporting.



Compliance and Other Matters

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

We noted certain matters that we reported to management of the University a separate letter dated January 31, 2013.

The University's responses to the findings identified in our audit are described in the accompanying schedule of findings and responses. We did not audit University's responses and, accordingly, we express no opinion on them.

This report is intended solely for the information and use of management, others within the entity, and the Government of the District of Columbia and is not intended to be and should not be used by anyone other than these specified parties.

KPMG LLP

January 31, 2013

Schedule of Findings and Responses
September 30, 2012

2012-01 Lack of Controls over the Implementation of the Banner System

Fiscal Year 2011 Condition:

During fiscal year 2011, the University implemented a new financial system, Banner. Based on a review of general information technology controls related to Banner, we noted the following during our fiscal year 2011 audit:

Banner Application Implementation and Program Change

- Several generic accounts were used during the Banner implementation to apply changes to the Banner application, operating system, and underlying database. Evidence of monitoring these generic accounts did not exist, and;
- Banner program changes were not consistently recorded to evidence the nature of such changes or testing activities. In addition, we did not observe any evidence of approvals of changes in accordance with a defined change management process.

Segregation of Duties – Banner Developers

- We noted that developers had access to the Banner production database. Specifically, two University employees, three Magic 10 consultants, and SunGard consultants had access to the Banner production database and were capable of making unauthorized changes to the data and schema of the database supporting the Banner system. Management did not have controls in place to monitor and document the activities of developers that had access to the production environment.

Banner Application Periodic Access Review

- Management had not implemented a formalized Banner application review process to determine whether Banner user access was commensurate with job responsibilities on an ongoing basis.

Fiscal Year 2012 Condition:

During our fiscal year 2012 audit, we noted that correction action was taken to mitigate certain control risks identified in the fiscal year 2011 audit; however, the following deficiencies continue to exist:

Banner Application Implementation and Program Change

- Policies and procedures related to generic account management originally defined by management during fiscal year 2012 did not include requirements for logging and monitoring of actions taken under generic accounts. As a result, a series of generic accounts with the ability to make changes, including nine accounts at the database layer, 19 accounts at the operating system layer, and 33 accounts at the application layer, held active access to the environment throughout fiscal year 2012. Of these accounts, a subset were tied to system processes and not procedurally logged into by end users while others were no longer necessary to exist within the environment, and;
- While a complete list of patches applied to the Banner application could be provided, changes impacting the functionality of the application made directly through the Oracle database during the period could not be produced in order to assess effectiveness of program change controls.

Segregation of Duties – Banner Developers

The access of the Magic 10 and SunGard consultants was revoked during fiscal year 2012; however the access of the two University developers, who are also the designated Database Administrators (DBAs) for Banner, was not able to be removed from the production database. Management implemented a policy requiring that the

Schedule of Findings and Responses September 30, 2012

individual responsible for developing the change would not be the same individual responsible for migrating the change; however the two developers with access to production remain able to circumvent this policy.

Banner Application Periodic Access Review

Management has implemented an access review process. However, this review process was not consistently performed or documented and was not comprehensive of the entire Banner user community.

Criteria:

Banner Application Implementation and Program Change

NIST SP 800-64, Security Considerations in the System Development Life Cycle, October 2008, states:

“An effective agency configuration management and control policy and associated procedures are essential to ensure adequate consideration of the potential security impacts due to specific changes to an information system or its surrounding environment.

Configuration management and control procedures are critical to establishing an initial baseline of hardware, software, and firmware components for the information system and subsequently for controlling and maintaining an accurate inventory of any changes to the system. Changes to the hardware, software, or firmware of a system can have a significant security impact.

Documenting information system changes and assessing the potential impact on the security of the system on an ongoing basis is an essential aspect of maintaining the security accreditation.”

Lastly, the Government Accountability Organization’s (GAO’s) *Evaluating Internal Controls in Computer Based Systems* (Black Book), 1981, states:

“Effective program change controls help maintain the integrity of applications and can be used to develop a list of changes which provide an audit trail of the computer-based system’s evolution. Even though these controls may frustrate programmers and sometimes cause delays in fixing applications, they are beneficial because they encourage data processing personnel to exercise more caution over changes to accepted production systems.”

Segregation of Duties – Banner Developers

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3, Recommended Security Controls for Federal Information Systems and Organizations, August 2009, section Access Control (AC-5) states:

“The organization:

- (a) Separates duties of individuals as necessary, to prevent malevolent activity without collusion;
- (b) Documents separation of duties; and
- (c) Implements separation of duties through assigned information system access authorizations.

Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, configuration management, quality assurance and testing, network security); (iii) security personnel who administer access control functions do not administer audit functions....”

Schedule of Findings and Responses September 30, 2012

Banner Application Periodic Access Review

NIST Special Publication (SP) 800-12, Revision 3, An Introduction to Computer Security: The NIST Handbook, October 1995 states:

“From time to time, it is necessary to review user account management on a system. Within the area of user access issues, such reviews may examine the levels of access each individual has, conformity with the concept of least privilege, whether all accounts are still active, whether management authorizations are up-to-date, whether required training has been completed, and so forth.

These reviews can be conducted on at least two levels: (1) on an application-by-application basis, or (2) on a system wide basis. Both kinds of reviews can be conducted by, among others, in-house systems personnel (a self-audit), the organization’s internal audit staff, or external auditors. For example, a good practice is for application managers (and data owners, if different) to review all access levels of all application users every month and sign a formal access approval list, which will provide a written record of the approvals. While it may initially appear that such reviews should be conducted by systems personnel, they usually are not fully effective. System personnel can verify that users only have those accesses that their managers have specified. However because access requirements may change over time, it is important to involve the application manager, who is often the only individual in a position to know current access requirements.”

Cause:

Based on a consideration of priorities and limited resources, management has not allocated the resources required to develop and implement a consistently applied change management process that mitigates the risks associated with, but not limited to, mitigating controls such as monitoring the activities of generic accounts and ensuring appropriate segregation of duties. Additionally, a formally documented change management process was not implemented by management for the Banner implementation, subsequent module implementations, and program changes.

Effect:

The lack of proper monitoring controls over generic accounts increases the risk that changes to application programs and data in the production environment may be applied that have adverse affects on the availability or processing/data integrity of the application without management’s awareness/approval. Also, without a formally documented change management process, there is an increased risk that change management procedures are performed inconsistently. As a result, unauthorized and/or invalidated changes may be implemented into the production environment that has adverse affects on the availability or processing/data integrity of the application. In addition, the lack of segregation of duties controls increases the risk that developers can create and apply changes to application programs and data to the production environment that have adverse affects on the availability or processing/data integrity of the application without management’s awareness/approval.

Lastly, by not performing a review of user accounts on a regular basis to determine whether access levels are appropriate for a given user’s job responsibilities and to verify that all user accounts belong to current employees, the following risks may exist:

- Employees may have access to the system that does not correspond with their current job responsibilities and/or may present a conflict of interest. This access could allow a person to advertently or inadvertently use various functions to alter the integrity of application data in an unauthorized manner.
- Should an active user account of a separated employee be present within the application, the separated person, with malicious intent, or another person with knowledge of this active user account, may have the ability to use this account to alter the integrity of application data in an unauthorized manner.

Schedule of Findings and Responses
September 30, 2012

Recommendation:

We continue to recommend that management implement the following actions:

Banner Application Implementation and Program Change

- Review and revoke access from any generic accounts no longer needed at the operating system, database, or application layers within the Banner environment. For those accounts that are required to remain active, management should implement a process to approve and document each use of the generic accounts in question and/or perform a periodic review of actions taken under these generic accounts.
- Configure settings or implement monitoring tools to log changes made to Banner application functionality, including key configuration changes.

Segregation of Duties – Banner Developers

- Implement logging and monitoring controls over the activities of the DBAs/developers. Documentation of these monitoring controls should be maintained and include sign-off from the independent reviewer, as well as notations regarding any activity regarded as an exception to University's policy related to change management and segregation of duties. Further, any suspicious activity, such as modifications to functionality or data without corresponding change request approvals, should be followed-up upon, as necessary.

Banner Application Periodic Access Review

Refine the current periodic access review process to include the following characteristics, which will strengthen it to consistently capture and remediate, in a comprehensive manner, cases of excessive access privileges stemming from either changes in job functions or unauthorized modifications to access rights:

- The review should be comprehensive of all user IDs with greater than read-only privileges to the application, which is performed quarterly or semi-annually depending on considerations such as:
 - (1) The volume of user access and likelihood of changes;
 - (2) The operation and strength of access controls around provisioning, de-provisioning, and management of changes for transfers; and,
 - (3) The relative risk of the system with respect to operational and financial importance to the company.
- The review should be conducted by business owners that are knowledgeable and can certify appropriateness of user access within the system and who do not also have access to modify users and privileges.
- The review should be based upon system-generated reports, even if these reports are re-formatted into Excel to facilitate the review process.
- The required changes resulting from the review should be remediated in a timely manner.
- The results of the review, including any required changes, should be documented for audit trail purposes.

Lastly, we recommend that these procedures be provided to and discussed with control performers. Further, management should monitor control performer adherence to the procedure on a periodic basis.

Schedule of Findings and Responses
September 30, 2012

Views of Responsible Officials:

There are factors that in our opinion should be considered in reviewing our response to the findings.

Banner Application Implementation and Program Change

Management concurs with this finding.

As it relates to the use and review of generic accounts, we believe we rectified the prior year findings based on previously-issued recommendations, and we have reviewed and revoked access to all generic accounts where the functionalities of Banner were not impacted.

We have also begun to perform a periodic review of actions taken under these generic accounts and will continue.

The Banner application is delivered with generic accounts that are required for baseline, and for its operation with its ancillary applications and services. Furthermore, additional generic accounts are used by the business units for the purpose of processing Banner “jobs” that are essential for batch processing. In these cases, the generic accounts do not have the privileges of updating any unique PIDM (student record). It should also be noted that business units own these generic units and control access to them and their use is outside of the purview of OIT. OIT has since removed generic accounts that are no longer being used or are no longer useful, and has been using the Track-it! System to log access to OIT controlled accounts at the database, application and OS levels.

As it relates to the recommendation to log changes to Banner, the recommendation listed may have legitimate rationale; however, could be functionally impractical depending on the scope of logging and monitoring performed. We will review options to log changes to specific tables and/or forms in Banner (as well as changes made by certain privileged or controlled accounts) in order to create an audit trail of data and configuration changes made to the system.

Segregation of Duties – Banner Developers

Management concurs with this finding.

We believe we have implemented policies and procedures that ensure a secure environment. We deploy *Track-it!*, an application that records change requests to the database from business units, and also tracks DBA’s access to the production environment. We also deploy *Project Insight* to tracks all approvals before execution.

We believe we rectified conditions as recommended in previous findings and we have mitigated the “*risk of changes to application programs and data and the configuration of the underlying database*” and its possible “*adverse affects on the availability or processing/data integrity of the application without management’s awareness/approval*”.

Banner Application Periodic Access Review

Management partially concurs with this finding.

We believe we have made considerable progress in rectifying issues listed in earlier findings and we have complied with most of the recommendations.

OIT has made significant efforts to ensure that the application security is reviewed and assessed periodically. Least privileged access continues to be the primary object in these exercises and business-unit owners are required to participate in the process. The University has faced tremendous turnover and transitions (e.g. Financial Aid Directors, Admissions Directors) which has limited OIT’s ability to perform the reviews on the schedule that

Schedule of Findings and Responses
September 30, 2012

KPMG deems suitable. Since the “stabilization” of the business unit leads, OIT has subsequently performed reviews and is and will continuously perform reviews that will be aligned with KPMG’s timing.

2012-02 Lack of Controls over the Financial Reporting Process

Condition:

In 2010, the District of Columbia Official Code 38-274.03 established a non-lapsing fund for the Higher Education Incentive Program Grant (HEIG) program. In fiscal year 2012, the District of Columbia Council included the current year funding of \$850,000 for the program within the University’s annual appropriation. The University did not spend the funds or incur any expenses related to the program during fiscal year 2012. However, to prevent the perceived loss of this funding, the University improperly recorded an unsupported manual journal entry to increase expenses and deferred revenues in the amount of \$850,000 into the general ledger. This entry was subsequently reversed prior to the issuance of the financial statements.

Criteria:

Statement of Financial Accounting Concepts No. 5, *Recognition and Measurement in Financial Statements of Business Enterprises*, states, ‘Expenses and losses are generally recognized when an entity’s economic benefits are used up in delivering or producing goods, rendering services, or other activities that constitute its ongoing major or central operations or when previously recognized assets are expected to provide reduced or no further benefits.’

The *District of Columbia Official Code 38-274.03, ‘Higher Education Incentive Grant Fund’* states, ‘There is established as a non-lapsing fund the Higher Education Incentive Grant Fund, which shall be a separate program line within the University of the District of Columbia budget. All funds deposited into the HEIG fund shall not revert to the unrestricted fund balance of the General Fund of the District of Columbia at the end of a fiscal year, or at any other time, but shall be continually available for the uses and purposes set forth in subsection (b) of this section without regard to fiscal year limitation, subject to authorization by Congress.’

Cause:

University management was attempting to show the grants funds as expended by recording an unsupported entry into the general ledger.

Effect:

Non-payroll operating expenses and deferred revenue were initially overstated by \$850,000 on the draft financial statements as of and for the year ended September 30, 2012.

Recommendation:

We recommend that management establish and implement policies and procedures to account for unused funds that are in accordance with generally accepted accounting principles. Additionally, we recommend that the University only record entries into the general ledger that represent an actual accounting transaction.

Views of Responsible Officials:

Management concurs with this finding.

Management agrees with the auditors’ recommendation to let this appropriated amount flow to the fund balance whenever the entire amount is not used for the required purpose by the end of each fiscal year. Furthermore, whenever there is a fund balance for this program, management will request additional budget authority in the following fiscal in order to accomplish the intent of the Council’s resolution.

Schedule of Findings and Responses
September 30, 2012

2012-03 Lack of Controls over Compliance with Investment Policy

Condition:

We noted that the University has \$1.76 million, or 4.6%, of its total investment portfolio invested in the alternative assets class with a single investment manager as of 9/30/2012. The amount exceeds the 3% limit for alternative investments held within a single investment manager, as noted in the Investment Policy, by 1.6% or \$617,000.

Criteria:

The *University of the District of Columbia Investment and Spending Policy*, Section IX-C states that “No more than 3% of the total market value of the endowment may be invested with any single fund manager in the alternative asset class.”

Cause:

As investment purchase and sale decisions are initiated autonomously by the respective fund managers, compliance can only be determined after purchase or sale. The University provides the Investment Policy to its fund managers and requests that the fund managers remain in compliance with the policy. However, University does not have adequate controls in place to monitor compliance.

Effect:

Non-compliance with the Investment Policy can subject the University to undue financial risk, tarnished public reputation, and legislative sanction.

Recommendation:

We recommend that management periodically review its investment portfolio, including the fund managers’ purchase decisions to ensure compliance with all Investment Policy requirements.

Views of Responsible Officials:

Management concurs with this finding.

Management has corrected the exposure issue by terminating the investment and moving the funds to a new investment manager.