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, 2013

CHARLES J. WILLOUGHBY
INSPECTOR GENERAL

OIG No. 14-1-11GG(a) **May 19, 2014**

May 19, 2014

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) 2013, 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 2013 (OIG No. 14-1-11GG(a)). This report sets forth KPMG's comments and recommendations to improve internal control and other operating efficiencies.

The report identifies three deficiencies considered to be material weaknesses. 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.

The three material weaknesses identified are: 2013-01, Lack of Controls Over the Implementation of the Banner System; 2013-02, Lack of Controls Over the Financial Reporting Process; and 2013-03, Lack of Controls Over Compliance With Investment Policy. Management responses are included in the report.

The results of tests performed by KPMG disclosed one instance of noncompliance or other matters required to be reported under *Government Auditing Standards* which is described in the schedule of findings and responses as item 2013-03.

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)
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
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)
Mr. Jeffrey DeWitt, Chief Financial Officer, Office of the 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)
Mr. Lawrence Perry, Deputy D.C. Auditor
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: Mark Stephenson (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: Chris Barkley (via email)
The Honorable Mark Begich, Chairman, Senate Subcommittee on Emergency Management, Intergovernmental Relations and the District of Columbia, Attention: Jason Smith (via email)
The Honorable Rand Paul, Ranking Member, Senate Subcommittee on Emergency Management, Intergovernmental Relations and the District of Columbia
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: Angela Ohm (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: Angela Ohm (via email)
The Honorable Barbara Mikulski, Chairwoman, Senate Committee on Appropriations, Attention: Kali Matalon (via email)

The Honorable Richard Shelby, Ranking Member, Senate Committee on Appropriations, Attention: Dana Wade (via email)
The Honorable Tom Udall, 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, in accordance with the auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States, the basic financial statements of the University of the District of Columbia (the University), a component unit of the Government of the District of Columbia, which comprise the statement of net position as of September 30, 2013, and the related statements of revenues, expenses, and changes in net position and cash flows for the year then ended, and the related notes to the basic financial statements, and have issued our report thereon dated February 4, 2014.

Internal Control Over Financial Reporting

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

Our consideration of internal control was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that were not identified. However, as described in the accompanying schedule of findings and responses we identified certain deficiencies in internal control that we consider to be material weaknesses and significant deficiencies.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A material weakness is a deficiency, or 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. We consider the deficiencies described in the accompanying schedule of findings and responses as items 2013-01, 2013-02, and 2013-03 to be material weaknesses.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the University's basic financial statements are free from 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 an instance of noncompliance or other matter that is required to be reported under *Government Auditing Standards* and which is described in the accompanying schedule of findings and responses as item 2013-03.

The University's Responses to Findings

The University's responses to the findings identified in our audit are described in the accompanying schedule of findings and responses. The University's responses were not subjected to the auditing procedures applied in the audit of the basic financial statements and, accordingly, we express no opinion on the responses.

Purpose of this Report

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

KPMG LLP

February 4, 2014

2013-01 Lack of Controls over the Implementation of the Banner System

During fiscal year 2011, the University implemented a new financial system, Banner. While improvements were made over general information technology controls related to Banner, we noted the following weaknesses continued to exist during our fiscal year 2013 audit:

Banner (and Supporting Infrastructure) Generic Accounts and Program Changes

During FY2012 testing, it was determined that policies and procedures related to generic account management originally defined by management during FY2012 did not include requirements for logging and monitoring of actions performed using generic accounts. As a result, a series of generic accounts with the ability to make changes, including 9 at the database layer, 19 at the operating system layer, and 33 at the application layer, held active access to the environment through FY2012. Of these accounts, a subset were tied to system processes and not procedurally accessed by end users while others were no longer necessary to exist within the environment.

During FY2013 testing, it was determined that procedures were defined and implemented to approve, log, and track the use of one of the accounts (BANSECR) with administrative access at the application and database levels. However, for two of five sampled uses of the account, both of which granted access to a consultant for application support, documented approval prior the implementation of the security changes by the BANSECR account was not evidenced.

Additionally, outside of this account, it was determined that a series of generic accounts with update or greater access within the environment, including 13 at the database layer, 16 at the operating system layer, and 30 at the application layer, did not have controls in place to either (a) log and monitor the activities taken under these accounts or (b) rotate the passwords on a periodic basis. A majority of these accounts were tied to system processes and not procedurally accessed by end users; however, 1 account at the database layer, 4 at the operating system layer, and 13 at the application layer were no longer required to be active within the environment. According to management, the passwords of these accounts were restricted to between 2 and 4 authorized members of the IT team. However, the lack of sufficient, documented controls over these generic accounts represents a weakness in the control environment that has not been fully remediated during FY2013.

Segregation of Duties – Banner Developers

During FY2012 test work, it was determined the two University developers served as the primary system administrators for the UDC production database supporting the Banner application. Management implemented a procedure requiring that the individual responsible for developing the change would not be the same individual responsible for migrating the change into production. However, the two developers retained access to migrate changes to production through administrative privileges on both the operating system and database supporting the Banner application. As a result, these developers were able to circumvent this procedure without detective controls to identify if such instances were to occur.

During FY2013 test work, per inquiry of management, it was determined that the extent of in-house development was minimal as the majority of changes applied to the application were provided as patches by the Banner vendor, Sungard. However, the combination of responsibilities and levels of access to the Banner environment held by these two individuals remained the same, and as a result, the segregation of duties issue represents an unremediated finding from FY2012.

Banner Application Periodic Access Review

During FY2012 test work, it was noted that throughout the stabilization period for Banner, IT personnel continued to work closely with business management to review and tailor access to the application based on the principles of least-privilege security. Additionally, management had implemented an access review process. However, this review process was not consistently performed or documented and did not include all Banner user IDs.

During FY2013 test work, stakeholders for each of the Banner systems were defined and access granted to the application objects under the stakeholder's purview was communicated in March 2013. However, as policies and procedures were not defined and documented to include documentation and timeliness requirements for the completion of the review, the review was not performed in a timely manner for certain Banner systems. One department completed the first review five months after the start of the process. The review was never completed for any other departments. As a result, this condition was determined to be unremediated from FY2012.

Criteria

Our internal framework for identifying and testing GITCs can be mapped to several commonly accepted information technology risk and control frameworks including those published by the National Institute of Standards and Technology (NIST), Information Systems Audit and Control Association (ISACA), and the International Standards Organization (ISO). For purposes of our reporting of findings for the University, we have provided below relevant criteria.

1. The Federal Information Security Management Act (FISMA), passed as part of the Electronic Government Act of 2002, mandates that Federal entities maintain IT security programs in accordance with NIST. The following NIST criteria were considered:
   a. NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook, October 1995;
   b. NIST SP 800-53, Revision 3, Recommended Security Controls for Federal Information Systems and Organizations, August 2009;
   c. NIST SP 800-64, Security Considerations in the System Development Life Cycle, October 2008; and
   d. NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology, September 1996.
2. The Information Systems Audit Control Association (ISACA) Control Objectives for Information and related Technology (COBIT®) 4.1, 2007.

Cause

Banner (and Supporting Infrastructure) Generic Accounts and Program Changes

Management's current periodic access review process does not include an evaluation of the necessity of active generic accounts managed by IT. As a result, the accounts that are no longer required to be active were not disabled.

Additionally, due to management's perception of the risk associated with generic/system accounts within the environment, management has not implemented controls to log and monitor activity taken them. Instead, management has deemed controls to restrict the knowledge of the password to a limited number of individuals to be sufficient to mitigate this risk. Additionally, as the majority of these accounts have not been procedurally accessed in the past, management did not believe the associated risk justified deploying resources and maintenance windows to rotate the passwords of these accounts.

Lastly, for the two noted cases in which approval was not documented prior to use of the BANSECR account, management considered the logging of the request from the third-party consultant as sufficient to address the risk of inappropriate actions being taken within the system.

Segregation of Duties – Banner Developers

Management has implemented a process to procedurally segregate the responsibilities for development and implementation into production for changes made to the database supporting the Banner application. However, management has not allocated the resources required to develop and implement change management controls that fully mitigate the risks associated with the condition including, but not limited to, the segregation of program development roles from production system administration roles among different individuals.

Banner Application Periodic Access Review

As policies and procedures for the Banner periodic access review were not defined to include requirements for the timely completion of and required documentation to support the review as well as ramifications of non-compliance, no escalation could be taken to ensure the completion of the review when initial responses were not received timely.

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.

Recommendation

We continue to recommend that management implement the following actions:

Banner (and Supporting Infrastructure) Generic Accounts and Program Changes

- Review and revoke access to any generic accounts no longer needed at the operating system, database, or application layers within the Banner environment. This process should be performed as a part of future periodic access reviews to ensure that access for these accounts continues to be required.

- Rotate the password for these shared accounts on a periodic and controlled basis, at least every 90 days. The password(s) should also be reset when an employee with access to the password(s) leaves the organization. Management should document and retain evidence of such password changes; or,

- Implement a process to approve and document each use of generic accounts and perform a periodic review of actions taken under these generic accounts in on a periodic and controlled basis. The review should be performed using a system-generated report of generic accounts accessed.

<u>Segregation of Duties – Banner Developers</u>

- Logical segregation of program development roles from production system administration roles among different individuals; or,

- 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.

<u>Banner Application Periodic Access Review</u>

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 University.

- 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.

Views of Responsible Officials

Management concurs with this finding.

2013-02 Lack of Controls over the Financial Reporting Process

Condition

During our audit, we noted that the University did not have adequate and effective internal controls in place over the financial reporting process as follows:

Lack of Controls over Litigation Contingencies

We noted that in fiscal year 2013, the University's initial litigation contingencies accrual represented 50 percent of the sum of the maximum ranges for cases with outcomes classified as both probable and reasonably possible, which is not in accordance with generally accepted accounting principles (GAAP).

The University's Office of the General Counsel (OGC) did not initially perform an analysis of legal cases sufficient to provide management with a reasonable estimate of legal losses. Cases were not properly classified in the legal response letter initially provided by the OGC. Notably, one case currently in arbitration was initially classified as reasonably possible with a range of $2.3 million to $4.5 million, but was later reclassified as probable with a range of loss of $2.6 million to $7.6 million, causing respective increases and decreases in the probable and reasonably possible categories and the accrual.

Inaccurate Accrued Leave Liability Balance

The University had an accrued leave balance of $3.8 million as of September 30, 2013. Per the D.C. Municipal Regulations, the University's leave accrual calculation should not include members of the teaching faculty. During our testwork over the accrued leave liability, we noted there were approximately 52 teaching faculty individuals for whom an accrual was calculated and included in the financial statements as of September 30, 2013. This resulted in an overstatement of approximately $177 thousand of the accrued leave liability as of September 30, 2013.

Unsupported Restricted Cash and Net Position Balances

The University reported approximately $650 thousand in restricted cash in note 3 to the basic financial statements. The University is unable to provide supporting documentation that this amount of cash is properly classified as restricted. Additionally, this balance was not reported as restricted on the statement of net position as of September 30, 2013.

The University reported approximately $187 thousand of restricted nonexpendable net position on the statement of net position as of September 30, 2013. The University is unable to provide supporting documentation that this balance is properly classified as restricted nonexpendable net position as of September 30, 2013. .

Unsupported Revenue Balances

Each year-end, in the preparation of its year-end financial statements, the University records accrued expenses for goods/services provided on or before September 30, based on inquiries with program officers and outstanding purchase orders. During the subsequent fiscal year, the difference between the actual amount paid and the accrued amount is recorded as prior year cost recovery revenue, along with a corresponding increase to contractual services expense. During our audit over other operating revenue, we noted that the University inappropriately recorded revenue in the current year for prior year cost recoveries in the amount of approximately $439 thousand. These amounts should have been recorded as a credit to current year expenses. As such, other operating revenue and contractual services expense were each overstated by this amount for the year ended September 30, 2013.

Inaccurate Grant Receivable Balances

During our audit of grant receivables, we noted that three grant balances within the grant receivable population had negative balances totaling approximately $334 thousand, which actually represented unearned revenue. As such, the ending balances of grants receivable and unearned revenue were understated by this amount as of September 30, 2013.

Criteria

In order to ensure financial information is useful in decision making and evaluating managerial and organizational performance, as well as demonstrating accountability and stewardship, controls must be properly designed, in place, and operating effectively to ensure that the University's accounting and financial information is fairly stated in accordance with GAAP.

As part of that requirement, there should be adequate controls in place over the processing of transactions recorded in the general ledger to prevent/detect a misstatement. Management is required to ensure amounts included in their general ledger represent valid and true transactions arising from the University's operations.

Cause

Adequate controls, policies, and procedures are not in place to ensure amounts in the University's financial statements are complete and accurate.

Effect

Material financial statement misstatements could go undetected.

Recommendation

We recommend that management establish and implement policies and procedures to ensure that amounts reported in the University's financial statements are complete, accurate, and represent actual and valid transactions arising from the University's operations.

Views of Responsible Officials

Lack of Controls over Litigation Contingencies

Management concurs with this finding.

During prior years financial statement preparation University management estimated its contingent liability by adding the minimum balances in both probable and reasonably possible categories of the estimated loss of the legal cases schedule obtained from Office of General Counsel (OGC).

During FY 2013 after examination of the open legal cases and extensive discussion with OGC, it was determined that neither the historical methodology nor the criteria prescribed by GASB Statement No. 62 resulted in an accrual amount that would reasonably represent the probable cost of resolving these legal cases. Further, if management did not take this conservative approach in calculating the accrued legal liability, inadequate resources would be set aside to cover future legal losses. Management believes that the amount accrued better reflects the cost associated with the probable outcome of these cases. However, we agree that our approach is not in compliance with GAAP and we continue to work with OGC to develop a schedule that represents the anticipated loss of future legal cases.

Inaccurate Accrued Leave Liability Balance

Management concurs with this finding.

Management recorded the accrued leave liability based on the data it received from Pay and Retirement Services. We acknowledge that UDC's management must work closely with the data providers to better ensure that the underlying data are accurate. Currently, UDC's HR and Pay and Retirement Services are working to rectify these discrepancies.

<u>Unsupported Restricted Cash and Net Position Balances</u>

Management concurs with this finding.

The balances in question did not change from previous audited fiscal periods and there were no issues raised about their presentation in the basic financial statements. Due to significant OCFO management turnover during the audit period, we are unable to provide additional support and/or explanation to validate these balances. In the absence of supporting documentation we believe that the best course of action is to concur with the auditors finding and make the necessary changes to future financial statement presentations.

<u>Unsupported Revenue Balances</u>

Management concurs with this finding.

Management agrees that the current method resulted in overstatement of income but implementation of this recommendation, leaving a negative expense in place, will result in the understatement of expenses for the fiscal year. In addition, leaving a negative expense increases the available budget of an account, which inevitably results in overspending. We will further examine this issue and develop and implement corrective actions that address the concerns listed above.

<u>Inaccurate Grant Receivable Balances</u>

Management concurs with this finding.

Management will implement additional controls to ensure that all grant receivable balances are periodically reviewed for accuracy and completeness. Any errors identified in the review process will be corrected in a timely manner for accurate presentation in the financial statements.

2013-03 Lack of Controls over Compliance with Investment Policy

Condition

The University had $37.8 million in its investment portfolio as of September 30, 2013. During our audit over the University's compliance with the University of the District of Columbia Investment and Spending Policy (Investment Policy), we noted that the University was noncompliant with the Investment Policy as of September 30, 2013 as follows:

- Within the University's fixed income investment portfolio, the University had $3.3 million invested in corporate bonds and $600 thousand invested in international bonds. Corporate and international bonds are not authorized fixed income investments per the Investment Policy.

- The University has $5.2 million, or 59.03%, of its fixed income investment portfolio invested in investments with a rating below an 'A' from a nationally recognized rating agency. Of this amount, $2.5 million in investments were not rated. The amount exceeds the Investment Policy's 25% limit, or $2.2 million, for fixed income investments rated below an 'A' by 34.03% or approximately $3 million.

- The University had $2.7 million, or 6.96%, of its total investment portfolio invested in the alternative assets class within a single fund manager. The amount exceeds the Investment Policy's 5% limit for alternative investments held within a single fund manager, by 1.96% or $753 thousand.

- The University has $12.5 million, or 29.38%, of its total investment and endowment funds invested in alternative trading strategies (limited partnerships). The amount exceeds the Investment Policy's 26% limit for alternative trading strategy asset class, by 3.38% or $1.44 million.

Criteria

The *University of the District of Columbia Investment and Spending Policy*, Section IX-B states that "Authorized fixed income investments are: U.S. government and agency bonds and notes, including convertible bonds and notes; municipal bonds and notes; and mortgage-backed securities."

The *University of the District of Columbia Investment and Spending Policy,* Section IX-B states that "Fixed income investments must be rated no lower than *"A"* by a nationally recognized rating agency. No more than 25% of the total amount of the investment and endowment funds invested in fixed income securities may be invested in securities rated below A. The 25% investment rating rule pertains only to all separately managed accounts as a whole."

The *University of the District of Columbia Investment and Spending Policy,* Section IX-D states that "Authorized alternative asset investments are private equity funds, buy-out funds, and hedge funds. No more than 5% of the total market value of the endowment may be invested with any single fund manager in the alternative asset class."

The *University of the District of Columbia Investment and Spending Policy,* Section VIII states that No more than 26% of the amount of the investment and endowment funds (at market value) may be invested in alternative trading strategies unless written approval is obtained from the CFO or his designee.

Cause

The University does not have adequate controls in place to monitor compliance with its investment policy.

Effect

Noncompliance 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 does not concur with this finding.

Management does agree that the investment policy was not clear in regards to corporate bond and international bond investment. The policy was re-drafted during the fiscal year and inadvertently the section related to corporate bonds and international bonds was removed in section IX. Those investments had previously been allowed under all the prior polices. That policy error will be corrected. Also the policy currently states that the investment allocation allows for up to 20% of the endowment investment in High Yield and Emerging Markets so this would cover corporate and international however section IX, part B. Fixed Income doesn't specifically state Corporate and International Bonds so the policy will be updated to clarify the confusion.

Management does not agree with the policy violation on investment below A rated. This aspect only applies to separate accounts and not all fixed income funds. Management will review the policy to make this issue more transparent.

Management disagrees with the finding that Limited Partnerships are always considered alternative investments. Alternatives should be determined by the type of strategy not the structure in which the investment is made. The funds in question invest in liquid, daily priced equities however the fund is not priced on available markets. The District invests in the same funds in other investment programs and was not treated as Alternatives. If these funds were not treated as alternatives this would not create violations in the single fund manager exposure or the asset class violation. We will review our policy position on Limited Partnership investments and how they should be treated going forward and will make policy revisions to address this position. Management is currently working on all the policy related issues and will be providing an updated policy for approval.