New York State Office of the State Comptroller
Thomas P. DiNapoli

Division of State Government Accountability

Controls Over CUNY Fully Integrated Resources and Services Tool

City University of New York

Report 2015-S-34 September 2016

Executive Summary

Purpose

To determine whether the City University of New York (CUNY) adequately controls access to the CUNY Fully Integrated Resources and Services Tool system (CUNYfirst) and whether CUNY adequately measured if users' needs were met. The audit covers the period January 1, 2013 through October 23, 2015.

Background

CUNYfirst, which replaced CUNY's Financial Management, Human Capital Management, and Campus Solutions applications, is an Enterprise Resource Program. The objective of CUNYfirst was to replace CUNY's legacy systems with an integrated and flexible state-of-the-art solution. During its early phases, CUNYfirst implementation was expected to be complete by 2012. By October 29, 2015, 20 campuses had at least part of the system implemented, and at that time, the projected date for project completion was October 2016. As of September 30, 2015, CUNY reported the cost to develop and implement CUNYfirst was $249.75 million.

CUNYfirst, like many large computer systems, uses role-based access. Roles are created for the various functions at CUNY, such as the Admissions Office or Registrar. These roles give individuals permission to perform certain operations that are assigned to these functions. For example, in the Admissions Office one of the roles would be to allow staff to update academic test data for a student. Students and staff are assigned particular roles, and thereby acquire the rights to access certain CUNYfirst applications.

As of April 23, 2015, CUNY reported CUNYfirst had approximately 1.27 million accounts (1.15 million students and 123,000 employees). The student accounts include both former and current students. The employee category includes faculty, administrative, and student employees whether active, inactive, or retired.

Key Findings

We concluded that CUNY's processes and controls did not adequately restrict CUNYfirst users' access to ensure that individuals only had appropriate roles assigned. For example, we determined that:

- CUNY's Central Office (CUNY Central) granted 60 roles to Application Security Liaisons, or ASLs (information technology personnel who grant access to CUNYfirst at the campuses) without adequate justification. The business needs for the ASLs to have the roles in question were unclear. In addition, there were 27 roles that were removed from employees who had left CUNY, but not until 3 to 32 months after their departure.
- A student had access to CUNYfirst Financial and Supply Chain Management (FSCM) module, a business application that students normally cannot access. Such access requires an approved access form; however, no form was on file for this student. The student, who was not an employee of the campus and had no business need for FSCM, could access FSCM data and accessed the FSCM application on three occasions. We also examined 244 employees' accounts, all of which

required approved access forms. We identified 170 employees who had 990 unauthorized roles, including 83 that were designated by CUNY as "sensitive." For example, certain users' roles allowed them to change personal information for any student, and this role was not restricted to the campus where the ASL worked.

- Multiple individuals appeared to have roles for which they had no business purpose. For example, 22 employees outside of financial aid could apply for student loans for individuals other than themselves. CUNY officials stated that while it may appear that these functions (such as applying for a loan) could be executed, they most likely could not. However, they provided no basis to support their statement. Also, a student employee had unauthorized grade change capability. For the period January through May 2015, this student employee changed grades 127 times for other students, but did not change her own grades.
- In 37 of 49 sampled cases, a user delegated a function to another person, but did not indicate an end date for the delegation. Without specifying an end date, the individual with delegated rights retains access indefinitely, increasing the risk of improper use.

Also, CUNY performed a survey of CUNYfirst users and potential users in November 2012 that did not include any students. Since then, another 11 campuses have implemented CUNYfirst; however, no survey or other process to obtain feedback from the users has been performed.

Our audit also identified certain findings and made a corresponding recommendation pertaining to the data integrity of particular CUNYfirst functions. We presented these findings and recommendation in detail to CUNY officials during the course of the audit's fieldwork. However, to help preserve security over these functions, we did not detail the findings and recommendation in this report.

Key Recommendations

- Require CUNY Central and the campuses to prepare and maintain documentation of all approvals of roles that are assigned or removed in CUNYfirst.
- Require CUNY Central, in addition to the attestations, to actively monitor all user access within CUNYfirst.
- Periodically review and adjust the user access roles in the system to meet the actual needs of the individuals identified in our audit and system-wide.
- Create a policy requiring a formal end and/or review date for all role delegations in CUNYfirst.
- Periodically survey users from all CUNYfirst user groups to measure whether their needs are being met.

Other Related Audits/Reports of Interest

City University of New York – York College: Time and Attendance Practices for Public Safety Staff (2013-S-65)

City University of New York – School of Professional Studies: Controls Over Bank Accounts (2014-S-78)

State of New York
Office of the State Comptroller

Division of State Government Accountability

September 2, 2016

James B. Milliken
Chancellor
City University of New York
205 East 42nd Street
New York, NY 10017

Dear Chancellor Milliken:

The Office of the State Comptroller is committed to helping State agencies, public authorities, and local government agencies manage their resources efficiently and effectively. By so doing, it provides accountability for tax dollars spent to support government operations. The Comptroller oversees the fiscal affairs of State agencies, public authorities, and local government agencies, as well as their compliance with relevant statutes and their observance of good business practices. This fiscal oversight is accomplished, in part, through our audits, which identify opportunities for improving operations. Audits can also identify strategies for reducing costs and strengthening controls that are intended to safeguard assets.

Following is a report of our audit of the City University of New York entitled *Controls Over CUNY Fully Integrated Resources and Services Tool*. This audit was performed pursuant to the State Comptroller's authority under Article V, Section 1 of the State Constitution and Article II, Section 8 of the State Finance Law.

This audit's results and recommendations are resources for you to use in effectively managing your operations and in meeting the expectations of taxpayers. If you have any questions about this report, please feel free to contact us.

Respectfully submitted,

Office of the State Comptroller
Division of State Government Accountability

Table of Contents

State Government Accountability Contact Information:
Audit Director: Carmen Maldonado
Phone: (212) 417-5200
Email: StateGovernmentAccountability@osc.state.ny.us
Address:
Office of the State Comptroller
Division of State Government Accountability
110 State Street, 11th Floor
Albany, NY 12236

This report is also available on our website at: www.osc.state.ny.us

Background

The City University of New York (CUNY) began in 1847 with the founding of the Free Academy by Townsend Harris. Over the decades, CUNY became a 24-campus university comprised of 11 senior colleges, seven community colleges, the Macaulay Honors College, and five graduate and professional schools, located throughout New York City's five boroughs. CUNY, the nation's largest urban public university, offers more than 1,400 academic programs, 200 majors leading to associate and baccalaureate degrees, and 800 graduate degree programs.

Although CUNY is considered a single integrated system, its legacy information technology systems were not integrated, and thus, these systems did not lend themselves to streamlining and standardization of business processes, such as Human Resources. Consequently, CUNY officials concluded that they needed to replace CUNY's financial, human resources, and student administration systems with an integrated and flexible state-of-the-art solution. According to CUNY's June 2006 Board minutes, CUNY decided to implement an Enterprise Resource Program system with the hope it would result in "maximizing computer functionality and access for students and prospective students, streamlining administrative applications throughout the University and effectuating cross-campus compatibility in computer hardware, software, applications and connectivity." At that time, CUNY sought to replace the "obsolete and homegrown systems with state-of-the-art functionality, an enterprise planning resource software solution..." The new system was named the CUNY Fully Integrated Resources and Services Tool (or CUNYfirst).

CUNY selected an end-to-end (the supplier of an application or a system provides all of the hardware, software, and resources and no other supplier is needed) higher education solution from Oracle, which included Oracle's PeopleSoft Enterprise Financial Management, Human Capital Management, and Campus Solutions applications, as well as Oracle Database. Oracle also provided certain consulting and hosting services.

The CUNYfirst system is made up of three modules, which perform distinct functions, detailed as follows:

- The Financial and Supply Chain Management module includes General Ledger, Procurement, Asset Management, and Budget and Planning functions;
- The Human Capital Management module includes Basic HR, Recruitment, Work Study Payroll, Employee Payroll, and Faculty Workload functions; and
- The Campus Solutions module includes Bursar, Admissions, Registrar and Financial Aid, Graduate Office, and Faculty Workload functions.

During its early phases, CUNYfirst implementation was expected to be complete by 2012. By October 29, 2015, 20 campuses had at least one module of the system implemented, and at that time, the projected date for project completion was October 2016. As of September 30, 2015, CUNY reported the cost to develop and implement CUNYfirst was $249.75 million.

CUNY Central's Office of Computing and Information Services (CIS) is responsible for providing

central support for CUNY's information technology and telecommunication needs. One of the key roles of CIS is to lead the development of CUNYfirst. Access security for CUNYfirst is maintained by the CIS's Information Security Department, which is headed by the Chief Information Security Officer (CISO). Each campus also has an IT Security Manager, who oversees local efforts to protect computing and information assets. Application Security Liaisons (ASLs) are the custodians of access to CUNYfirst. At the time of our audit, there were 89 ASLs designated at 22 CUNY campuses. CUNY's Central Office (CUNY Central) also has an ASL who, in addition to CUNYfirst custodial duties, handles highly sensitive access matters CUNY-wide. The ASLs are chosen by the campus Chief Information Officers and must be full-time employees.

There were approximately 1.27 million CUNYfirst accounts as of April 23, 2015 (1.15 million students and 123,000 employees). The student accounts include both former and current students. The employee categories include faculty, administrative, and student employees, who were active, inactive, or retired.

Audit Findings and Recommendations

CUNY has policies and procedures in place for granting access to CUNYfirst once a school goes live in the system. However, we determined that CUNY Central and the campuses did not always comply with the requirements to ensure that only persons requiring particular roles were authorized for those roles. In addition, CUNY's monitoring of users' access and roles was inadequate. Also, CUNY performed a survey of CUNYfirst users and potential users in November 2012 that did not include any students, the largest group of users. Since then, another 11 campuses have implemented CUNYfirst, but no survey or other process to obtain user feedback has been performed. We recommend that CUNY improve its controls over access by enforcing documentation requirements and improving monitoring of access controls. In addition, CUNY should periodically survey all user groups to measure whether users' needs are being met.

General Access

Oversight and Monitoring by CUNY Central

CUNYfirst, like many large computer systems, provides users with role-based access. Roles are created for the various functions at CUNY, such as the Admissions Office or Registrar. In CUNY's case, these roles would give individuals permission to perform certain operations that are traditionally assigned to these functions. For example, in the Admissions Office, one of the roles allows staff to update students' academic test data. Students or employees (or other system users) are assigned particular roles, and through these assignments, acquire the rights to perform particular functions.

During roll-out of CUNYfirst to the campuses, mass uploads of credentials for employees and students were performed by CUNY Central. In addition, CUNY Central grants and removes access to ASLs at each campus and performs a periodic clean-up of access permissions. We reviewed documentation for 124 of these roles and determined that it was insufficient for 104 (84 percent) of them. Officials explained that 60 of these roles were assigned when certain schools went "live" with CUNYfirst. However, to support these actions, CUNY merely provided a list of names with some limited cryptic comments. There were no contemporaneous documents to support the need for these individuals to be assigned these particular roles. Further, 27 of the 104 roles represented access for employees who had previously left CUNY employment. While access to these roles (or applications) was eventually removed, it was often not done in a timely manner. We determined that the roles were removed from 3 to 32 months after their departure.

After roll-out, CUNY Central monitors campus activity through an annual control self-assessment review (referred to as an attestation). A control self-assessment is a process where staff in a business unit attest to the controls in place within their unit. CUNY commonly uses control self-assessments when deficiencies are detected in critical controls at the campuses, and CUNY Central requires corrective action plans to remediate the deficiencies and provide for follow-up. For example, as part of the Analysis and Testing of Controls process, each campus must review certain users' access roles to ensure a separation of duties between the procurement and accounts payable

functions. Separation of duties is one of the most important features of an internal control plan and is critical to decreasing fraud as well as detecting and correcting innocent errors. When we reviewed the attestations received by CUNY Central for spring 2015, we identified 47 individuals who had incompatible roles in the procurement and accounts payable functions. However, there was no evidence that CUNY Central followed up to determine if corrective actions were taken or compensating controls were implemented.

Role Access and Sufficiency of Approvals

Student CUNYfirst access is automatically provisioned and made available when a student first signs in to his/her account. For employees, access can be granted in two ways: by completing a user access form for individuals or bulk load requests of six or more staff; and through CUNY Central for mass changes. Both students and employees have standard access roles in the system. For example, one of the initial access roles provides self-service capabilities for both groups. This allows them to edit limited information in their personal profile. Students are normally provided two base roles, while employees are provided four and faculty five base roles.

CUNY's Guidelines for Requesting CUNYfirst Application Security Access state that employees (including students who are employed on campus) requiring additional access to perform their jobs must submit a completed access form, with the necessary approvals. An appropriately approved form is signed by an employee, supervisor, and the Subject Matter Experts (SMEs) in each department. The form is then sent to the help desk at the campus or the CIS Service Desk at CUNY Central. The ASL processes access for all completed, approved, and logged forms. Forms that do not have the appropriate approvals will not be processed.

During our audit survey, we selected an initial judgmental sample of 23 accounts. We found that 14 of 23 users sampled were provided access despite the lack of required approval signatures. One of the 14 users was a student account with more than the standard student access, which therefore required an approved access form. However, no form was on file for this student. This student, who was not an employee of the campus and had no need for the Financial and Supply Chain Module (FSCM) data, could access FSCM data and accessed the FSCM application on three occasions. Further, this student was granted rights to change financial data, which included certain confidential data. FSCM access should be restricted to specific financial management employees and is not normally assigned to students. In response to our preliminary findings, CUNY officials told us that CUNY terminated this student's FSCM access.

Based on our survey results we expanded our testing and selected a statistical sample of 306 accounts out of the population of 1.27 million accounts to test CUNYfirst access at 22 CUNY campuses. Due to the high proportion of students to employees, this sample was predominately students. We therefore selected an additional random sample of 217 employees. In total, we tested 279 student accounts and 244 employee accounts.

We determined that 126 (51.6 percent) of the 244 employee accounts were not properly approved. The 126 accounts had 192 forms that lacked certain required sign-offs, while two accounts had no form on file whatsoever. Moreover, ten of the forms were signed and approved by the same

employee. Of the 126 employee accounts that lacked proper approvals, 119 accounts had more than standard CUNYfirst access as well, including the two employees with no approval forms. Altogether, we found 990 roles that were not properly authorized, and 83 of these were deemed "sensitive" by CUNY. Examples of these roles included the ability to change personal information for any student and the ability to access information at campuses other than the campus at which the ASL worked.

In response to our preliminary findings, CUNY informed us that all Campus ASLs will be directed to ensure that requirements for access are enforced. In addition, CUNY campuses rescinded access for two individuals, provided additional forms that were not located during our visits, and prepared forms for the roles assigned to six of the selected employees. Of the 279 student accounts we reviewed, none of them had more than the standard CUNYfirst access roles.

Access Functionality

The primary users of the Campus Solutions module are the Bursar, Admissions, Registrar, Financial Aid, and Information Technology departments. Collectively, the heads of these departments are called the "BARFIT" group. During our meetings with the university BARFIT members, we were informed that there are instances where individuals in one group may need "read only" access to view information from another group, with no need to change the other group's data.

However, during our campus visits, we found that 25 of 100 individuals we observed had access that appeared to exceed their business needs. For example, 22 employees outside of financial aid had the ability to apply for student loans for individuals other than themselves. CUNY officials stated that while it may appear that these functions could be executed, they most likely could not. However, officials provided no documented evidence to support their belief.

Also, we found one student employee who had unauthorized grade change ability at the school the student attended. CUNY's policies do not allow students or part-time employees to access non-public information, such as grades or personally identifiable information, unless an approved waiver is in effect. However, we determined that a student, who was a part-time employee in the Registrar's Office, had the ability to change grades. According to the Registrar, this student employee should not have had access to the grade change function. A grade change report for the period January through May 2015 revealed that this employee changed grades 127 times for other students; however, she did not change her own grades. In response to our preliminary finding, the college modified the profile for this student to eliminate grade change access. However, even if allowed by the waiver process, we question grade change authority being granted to students due to the potential risk it presents.

Our audit also identified certain findings and made a corresponding recommendation pertaining to the data integrity of particular CUNYfirst functions. We presented these findings and recommendation in detail to CUNY officials during the course of the audit's fieldwork. However, to help preserve security over these functions, we did not detail the findings and recommendation in this report. Subsequent to the report's issuance, we will follow up with CUNY officials to assess their progress with efforts to address the detailed findings and recommendation in question.

Recommendations

1. Require CUNY Central and the campuses to prepare and maintain documentation of all roles that are assigned or removed in CUNYfirst.

2. Require Cuny Central, in addition to the attestations, to actively monitor all user access within CUNYfirst.

3. Periodically review and adjust the user access roles in the system to meet the actual needs of the individuals identified in our audit and system-wide.

4. Ensure that ASLs grant access only upon receipt of a fully approved form.

5. Implement a practice that requires student employees to document all grade changes processed and document the review of these changes.

Self-Assigned Access

As noted previously, ASLs are the custodians of access to the CUNYfirst system. As such, ASLs not only have the authority to grant or remove access for any user within their campus jurisdiction, they can also grant or remove access for themselves. In fact, we found that 24 ASLs CUNY-wide adjusted their own access 482 times between January 2013 and August 2015 without formal supervisory approval. Further, during the same period, there were 20 individuals who were not ASLs, but nonetheless adjusted their own CUNYfirst access 32 times. In 30 cases, these individuals added roles for themselves.

In response to our preliminary finding, CUNY officials stated that in most instances ASLs assigned additional roles to themselves to help assess the functionality of a particular role and its limitations before granting users requested access. Officials added that this process enabled ASLs to intelligently advise SMEs about their various access requests. Generally, it was expected that ASLs would rescind their access after they completed assessments of the roles requested by other users.

We found, however, that of the 482 self-assigned roles, only 150 were to remove certain CUNYfirst access, despite CUNY's claim that most role adjustments were primarily for testing purposes. Over 250 of these self-assigned accesses lasted longer than one week, and some were never removed. For example, one ASL assigned himself a role in March 2013, and as of July 2015 (nearly two and half years later), the role had not been removed. In response to our preliminary observations, CUNY listed five action steps they were planning to take to strengthen the controls over this process, including research of a PeopleSoft control that would prevent ASLs from self-assigning access.

Recommendation

6. Create a control within the CUNYfirst system that prohibits ASLs and other users from changing their own access roles.

Delegated Access

CUNYfirst allows supervisory delegation of certain CUNYfirst functionality. This gives supervisors the ability to delegate some of their access to other staff members within the Human Capital Management module. Delegation, as described by CUNY officials, is the process where one person authorizes another to serve as his or her representative for a particular workflow task or responsibility as their "proxy." This type of delegation is normally a three-part process wherein: the supervisor creates an electronic request; the proxy accepts (or declines) the request; and when the delegated access is no longer needed, the supervisor revokes the request. Per CUNY officials, the supervisor should include both a start and end date when creating a delegation request. The termination of the delegated access can also be performed by an ASL.

We reviewed 49 cases where representatives delegated a workflow task to a proxy. However, for 37 (75.5 percent) of the selected cases, the supervisor did not include an end date for the delegation period. According to CUNY officials, although the roles are delegated to an individual, any work that is performed by that person will be reviewed as part of the standard workflow process. However, roles and access for standard work flow activities should be granted through the prescribed review and approval process, as detailed previously in this report. Moreover, by failing to provide an end date for a delegated task, there is a lack of adequate control over the function in question. Further, if a supervisor leaves CUNY prior to terminating delegated roles, the individual who was delegated access could potentially retain such access indefinitely. This could increase the risk of inappropriate data entries or changes.

Recommendations

7. Create a policy requiring a formal end and/or review date for all role delegations in CUNYfirst.

8. Require long-term access roles to be granted through the standard review and approval process.

Survey of User Needs and Opinions

CUNY acknowledges that students, faculty, and staff are the primary users of the CUNYfirst system. CUNY's stated mission for the CUNYfirst Project includes the desire for the system to "Improve decision making," "Enhance end-user communication, operational efficiencies and productivity," and "Enhance delivery to students, faculty and staff." To assess whether or not the system meets these goals, feedback from a cross section of key users is critically important.

CUNY started implementing the CUNYfirst system in phases, beginning late in 2010. By summer

2012, nine schools were using at least one module of the system. In November 2012, CUNY surveyed 7,564 non-self-service users and academic officers (Presidents, VPs, Deans, and Department Chairs), but no other faculty, to obtain feedback and measure reactions to the system. No students were included in the original survey sample. Some individuals who were surveyed were users of the system, and others were potential users.

The survey results indicated that users of the system had a more favorable opinion than potential users. Faculty members, however, were generally critical of the system and referenced several issues they believed were in need of attention. For example, faculty identified the need for better training and communication about the system. Since that survey, 11 campuses have been added; however, CUNY has not used further surveys or other methods to obtain feedback on CUNYfirst. Consequently, CUNY has limited feedback to assess how new users and students view CUNYfirst and to identify issues that could require remediation.

Recommendation

9. Periodically survey users from all CUNYfirst user groups to measure whether their needs are being met.

Audit Scope and Methodology

We conducted this audit to determine whether CUNY ensures that only persons actually needing access to CUNYfirst are granted such access. The audit also sought to determine whether CUNYfirst met the needs of its users. The audit covered the period from January 1, 2013 through October 23, 2015.

To accomplish our objectives, we reviewed policies, procedures, and guidelines related to user needs, access control, and security regarding the CUNYfirst system. We interviewed CUNY's officials and employees to obtain an understanding of the internal controls related to CUNYfirst. We observed users, analyzed the documentation of user access, and reviewed and analyzed reports generated by the CUNYfirst system.

We went to 22 campuses and requested screenshots of the actual access in all modules of the CUNYfirst system and all forms on file for these individuals in order to conduct our testing. For the first test, we compared the access from the screenshots to the access granted by automatic provisioning upon claiming accounts, initial provisioning of the systems, and forms. The second test looked at each form to ensure that it was properly approved. In cases where the supervisor is the SME, we found these to be properly approved. Initially, we selected a judgmental sample of 23 accounts to review, and subsequently we expanded the sample as warranted.

We also selected a statistical sample of 306 accounts out of the population of approximately 1.27 million accounts to test access at the 22 CUNY campuses where CUNYfirst was operational. Further, we randomly selected a judgmental sample of 217 accounts from the files at 22 campuses. We judgmentally sampled between eight and ten forms, or help desk case numbers from the files

found at each campus to be tested in the same way as our statistical sample. In addition, we performed observations of 100 users' accesses during our visits to campuses.

We conducted our performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

In addition to being the State Auditor, the Comptroller performs certain other constitutionally and statutorily mandated duties as the chief fiscal officer of New York State. These include operating the State's accounting system; preparing the State's financial statements; and approving State contracts, refunds, and other payments. In addition, the Comptroller appoints members to certain boards, commissions, and public authorities, some of whom have minority voting rights. These duties may be considered management functions for purposes of evaluating organizational independence under generally accepted government auditing standards. In our opinion, these functions do not affect our ability to conduct independent audits of program performance.

Authority

This audit was performed pursuant to the State Comptroller's authority under Article V, Section 1 of the State Constitution and Article II, Section 8 of the State Finance Law.

Reporting Requirements

We provided a draft copy of this report to CUNY officials for their review and comment. We considered their comments in preparing this final report and attached those comments in their entirety at the end of it. In their response, CUNY officials generally agreed with our recommendations and indicated certain steps that have been and will be taken to address them. Our rejoinders to certain CUNY comments are included in the report's State Comptroller's Comments.

Within 90 days after final release of this report, as required by Section 170 of the Executive Law, the Chancellor of the City University of New York shall report to the Governor, the State Comptroller, and the leaders of the Legislature and fiscal committees, advising what steps were taken to implement the recommendations contained herein, and where recommendations were not implemented, the reasons why.

Contributors to This Report

Carmen Maldonado, Audit Director
Abe Fish, Audit Manager
Daniel Raczynski, Audit Supervisor
Anthony Belgrave, Examiner-in-Charge
Jasbinder Singh, Senior Examiner
Rahul Singh, Senior Examiner

Division of State Government Accountability

Andrew A. SanFilippo, Executive Deputy Comptroller
518-474-4593, asanfilippo@osc.state.ny.us

Tina Kim, Deputy Comptroller
518-473-3596, tkim@osc.state.ny.us

Brian Mason, Assistant Comptroller
518-473-0334, bmason@osc.state.ny.us

Vision

A team of accountability experts respected for providing information that decision makers value.

Mission

To improve government operations by conducting independent audits, reviews and evaluations of New York State and New York City taxpayer financed programs.

Agency Comments

The City University of New York

Office of Internal Audit and Management Services
230 West 41st Street, 11th Floor
New York, NY 10036
Tel: 646-664-3090
Fax: 646-664-3219

July 18, 2016

Ms. Carmen Maldonado
Audit Director
Office of the State Comptroller
Division of State Government Accountability
59 Maiden Lane - 21st Floor
New York, NY 10038

Re: Draft Audit Report# 2015-S-34--
Controls over CUNY Fully Integrated
Resources and Services Tool

Dear Ms. Maldonado:

We appreciate the opportunity to respond to the above-referenced draft report on OSC's audit of CUNYfirst system controls. The complexity of the audit, as reflected by the breadth of the report, only hints at the vast undertaking the CUNYfirst project represents. CUNYfirst was born out of the necessity of replacing aged, unreliable, and often incompatible systems spread out across the University's many campuses in favor of a state-of-the-art integrated system to manage effectively and efficiently the imperatives of over 1.2 million system users. These users comprise students, college applicants, faculty, administrators, and may others—both active and inactive in the system.

CUNYfirst is constructed on an Oracle/PeopleSoft platform, the same platform, incidentally, that the major New York State and New York City government administrative systems are built on. Because the system uses current technology and is compatible with those of our state and local governments, the transformation represented by CUNYfirst has helped ensure that CUNY's ability to provide first-rate service levels to its many constituents will be preserved for generations to come.

Before responding to the recommendations made in the report, we wanted to add some clarification and correct some of the representations made by the auditors in various sections of the report:

General Access

CUNYfirst Application Security Liaisons (ASL's) are designated individuals at every CUNY college and the Central Office who receive training and authorization to assign a limited set of

INVEST IN CUNY

CUNYfirst non-administrative (from a PeopleSoft perspective) access roles. The set of roles that ASL's are able to assign are further limited to roles that business process owners have deemed appropriate to be assigned to campus users and that do not require approval by the Central Office or the business process owner themselves. ASL's are so designated by a signed approval from a campus executive (nominally by the campus Chief Information Officer or Vice President for Administration).

The CUNYfirst Application Security Liaison function is authorized to assign any non-restricted role to a user having the required approval. This scope of authorization is inherent to the designation of an individual as an Application Security Liaison.

To maintain an orderly role assignment process during the phased implementation of CUNYfirst across the campuses, CUNY determined that it would further restrict ASL role assignment capability. This additional restriction prevented ASL's at a particular campus from assigning roles pertaining to CUNYfirst functions that were not yet active for their campus.

This additional restriction was implemented by reducing the default set of roles an ASL can assign and creating granular ASL security roles by functional area to add back the capability when desired. The new security roles were progressively assigned to ASL's at the functional go-live for their campus, enabling subsequent assignment of roles to users relevant to the functional area of CUNYfirst.

Questioned by OSC in this section is the documentation of the assignment of these granular, functional ASL security roles. Since, as stated above, ASL's are authorized to assign any non-restricted role to a user having the required approval, there was no need for an additional documented approval process authorizing the assignment of these ASL security roles at this stage. Instead, as part of routine pre-go-live preparation, the implementation team assigned the applicable functional security roles to the then-current ASL's at the campus to support their go-live.

* Comment 1

In response to the request for documentation of the ASL role assignments, CUNY provided work files and/or communications used by the implementation team to perform go-live support activity.

It is notable that the implementation of the additional restrictions enhanced security by helping to keep role assignment aligned with go-live timelines, reduced complexity and avoided exceptions when user-level roles were batch-assigned as part of campus go-live activity through approved user access matrices.

With respect to the auditors' finding that "27 of 104 roles [deemed to have insufficient documentation] represented access for employees who had previously left CUNY employment," the procedure to remove access from an individual requires that the campus create a service ticket containing an authorized approval for access to be removed. In the cited instances the procedure was not initiated. A significant mitigating factor is that CUNYfirst automatically disables an employee account when there is no active job record (e.g., a separated employee), ultimately preventing a former employee from accessing CUNYfirst.

* Comment 2

*See State Comptroller's Comments, page 22.

CUNY has re-emphasized to campuses the need for ASL access to be removed when an ASL separates from CUNY. CUNY will review and affirm ASL access with the campuses on a periodic basis.

Due to variations in the organization of campus functional units, it is infeasible for the CUNYfirst system itself to detect incompatible functional roles with regards to appropriate segregation of duty. The CUNYfirst access approval process relies fundamentally on functional unit heads ("Access Approvers") and Business Process Owners to determine whether a particular access request is contextually appropriate.

* Comment 3

Role Access and Sufficiency of Approvals

With respect to the student found to have access to the CUNYfirst Financials Supply Chain Module (FSCM), CUNY concurs that an individual student was inadvertently and inappropriately assigned access to FSCM. CUNY believes, however, that OSC extrapolated beyond its available evidence when it states that the student "accessed FSCM data." The FSCM audit trail entries provided signify that the student accessed the FSCM *application*. This could have occurred if the student merely clicked on an FSCM link within CUNYfirst.

* Comment 4

There is no evidence available with which OSC could corroborate to conclude that the student accessed FSCM data. Further, based on a lack of transactional logs, there is positive validation that no FSCM transactions occurred. CUNY will periodically review student access to FSCM.

Access Functionality

With respect to the finding that "22 employees outside of financial aid had the ability to apply for student loans for individuals other than themselves," the CUNYfirst Campus Solutions Student Center function is PeopleSoft delivered functionality that allows authorized college and university personnel within administrative units (e.g., registrar, bursar, admissions, etc.) to be able to visualize, from a student's perspective, certain CUNYfirst functions virtually. This feature aids and facilitates individualized student assistance and counseling by staff in those units.

Though it may appear that Student Center access allows a student loan application to be initiated through this feature, the ability to do so was not verified. Even if an application could be initiated, a safeguard exists to detect and prevent unauthorized direct loan applications. A query has been enhanced to identify the person who submitted the loan request. During loan application review, a financial aid officer can determine if the application was not initiated directly by the student, triggering additional review and authentication of the request.

Since transactions cannot be entered into the production CUNYfirst system for audit verification purposes, CUNY suggested that OSC witness whether a student loan application could be successfully initiated in a non-production, test environment. OSC declined.

* Comment 5

Delegated Access

CUNY restates that it is delivered PeopleSoft functionality to permit certain HCM workflow capability to be delegated by a supervisor. Access roles are not delegated.

With respect to the risk associated with supervisors who leave CUNY prior to terminating delegated access to another individual, though an existing HCM workflow delegation is not

automatically invalidated when an employee separates from CUNY, Human Resources personnel actively participate in these workflows and evaluate and must approve all transactions. Human Resources can question or reject a transaction if an inappropriate delegation is observed.

The report also states that an ASL can terminate delegated access. Though an ASL can remove the associative role(s) that enable access required by the PeopleSoft HCM delegated workflow function and hinder its ability to function correctly, such removal is not equivalent to terminating the delegated workflow itself. ASL's do not have access to the HCM delegated workflow function solely by means of their ASL status.

The following represents CUNY's responses to the several recommendations outlined in the draft report:

Recommendations

Recommendation

1. Require CUNY Central and the campuses to prepare and maintain documentation of all roles that are assigned or removed in CUNYfirst.

University Response

CUNY agrees with this recommendation

Recommendation

2. Require CUNY Central, in addition to the attestations, to actively monitor all user access within CUNYfirst.

University Response

CUNY agrees with this recommendation with the one qualification that the primary responsibility for continuous monitoring of user access will rest with the college functional unit heads, as they are better suited to making the timely determination that an employee's duties may have evolved to a point where such duties have become incompatible with the employee's access privileges.

Recommendation

3. Periodically review and adjust the user access roles in the system to meet the actual needs of the individuals identified in our audit and system wide.

University Response

CUNY agrees with this recommendation.

Recommendation

4. Ensure that ASL's grant access only upon receipt of a fully approved form.

University Response

CUNY agrees with this recommendation and will work to ensure that the protocols requiring signed user access approval forms are observed in all instances.

Recommendation

5. Implement a practice that requires student employees to document all grade changes processed and document the review of these changes.

University Response

CUNY agrees that there are particular risks associated with providing student employees with certain access to sensitive information and giving such employees write-access to certain system functionality. CUNY's IT Security Procedures require that part-time employees (e.g., student employees, or college assistants) may only be granted access beyond self-service access upon the issuance of a waiver. If such a waiver is granted, the same internal controls and monitoring protocols that apply to any user given system access apply to these part-time employees, and no user should have the ability to perform any part of a grade change transaction without authorization. All transactions are expected to be reviewed to ensure all authorizations were received.

Recommendation

6. Create a control within the CUNYfirst system that prohibits ASL's and other users from changing their own access roles.

University Response

CUNYfirst Application Security Liaisons (ASLs) are designated individuals at every CUNY college and the Central Office who receive training and authorization to assign a limited set of CUNYfirst non-administrative (from a PeopleSoft perspective) access roles. The set of roles that ASL's are able to assign are further limited to roles that business process owners have deemed appropriate to be assigned to campus users and that do not require approval by the Central Office or the business process owners directly.

In OSC's testing to validate that requested roles are assigned with the least amount of privileges required by an individual to perform their job function, OSC found that some ASLs would assign an additional role or set of roles to their own account. CUNY determined that in most instances ASLs were assigning additional roles to themselves as a means of analyzing the functionality of a particular role and its limitations before granting requested access to a user. This procedure enables the ASLs to intelligently advise subject matter experts against improvident access requests. However, in order to further strengthen the controls over the process, the University has taken the following actions:

* Comment 6

1. ASL's have been instructed to perform role analysis in a non-production, simulation environment only.

2. Should ASL's require additional access in production for any reason, ASL's will follow the standard access approval process. Once approved by a business process owner, such access will be assigned to them in the production system by another ASL.

3. The ASL Handbook and training materials is being updated to document the above requirements.

4. A query will be developed to identify ASL self-assigned role activity to be reviewed by campuses with compliance documented in their bi-annual attestation.

5. A PeopleSoft control that would prevent ASL's from self-assigning any access to themselves is under research.

Recommendation

7. Create a policy requiring a formal end and/or review date for all role delegations in CUNYfirst

University Response

CUNY's general policy is to grant users with only as much access to system functionality as required while assuming any particular user role. CUNY agrees that there were isolated occurrences where access delegation was not rescinded in a timely manner once it was no longer necessary for a user to have such delegated access. CUNY will improve monitoring to ensure that delegated access is appropriately removed if the nature of the delegation does not lend itself to the predetermination of an end date.

Recommendation

8. Require long-term access roles to be granted through the standard review and approval process

University Response

CUNY disagrees that this recommendation is practicable. A fundamental characteristic of PeopleSoft Human Capital Management (HCM) is that organizational hierarchies are defined and then configured into HCM. Access to HCM functions are then permitted on the basis of an individual's position and status.

Since HCM workflows are commonly carried out by non-supervisors (e.g., administrative assistants), whose position definition within CUNYfirst does not permit access to the Manager Self-Service function, delegation is the only means to accomplish establishing this capability within the system.

* Comment 7

Recommendation

9. Periodically survey users from all CUNYfirst user groups to measure whether their needs are being met

University Response

CUNY has been consulting with various user groups on the development of an effective means of soliciting user feedback in our University setting. Such consultations have included discussion of email surveys and other methodologies that would be designed to elicit as high a number of responses as would be useful and informational.

Again, thank you for the opportunity to respond to the audit. If you have questions or need additional information, please do not hesitate to contact me.

Very truly yours,

Gordon Taylor
Executive Director

cc: Chancellor James B. Milliken
Executive Vice Chancellor and COO Allan H. Dobrin
Vice Chancellor and CIO Brian T. Cohen

State Comptroller's Comments

1. In response to our draft report, CUNY officials assert that there was no need for documentation to authorize the assignment of the additional granular, functional security roles to ASLs as part of CUNYfirst's pre-go-live campus preparations. We believe, nonetheless, that CUNY officials should review this issue and establish a formal procedure that clearly identifies when documented approval is required to assign ASL security functionality (roles), as well as a process to document exceptions to this procedure.
2. CUNY officials stated that "CUNYfirst automatically disables an employee account when there is no active job record." However, officials did not provide any support that the three employees, who left CUNY employment and were assigned 27 CUNYfirst roles, had their access capabilities disabled timely or at all, as detailed in the report.
3. Our report does not state that the CUNYfirst system should detect incompatible functional roles with regard to proper segregation of duties. In fact, our report notes that we found 47 individuals who had incompatible roles, but there was no evidence that CUNY Central officials determined if corrective actions were taken and/or compensating controls were implemented to address the incompatible roles.
4. We acknowledge that there was no definitive evidence that the student actually accessed FSCM data. Nevertheless, there was material risk that the student could have accessed such data, due to the weakness detailed in the report. Although FSCM's audit trail entries indicated when FSCM data was edited, those entries did not indicate when FSCM data was accessed, but not edited. Further, we amended our report as appropriate to improve the technical presentation of this matter.
5. We acknowledge that OSC auditors declined use of the test environment. The reason for that declination, however, was absent from CUNY's response. In fact, OSC auditors declined use of the test environment because there was limited assurance that the application's initiation (within the test environment) would be performed in the same manner as it was in the live CUNYfirst system.
6. While CUNY stated that ASLs assigned the additional roles to themselves to analyze the roles' functionalities, as stated in the report, we found that 250 roles were self-assigned for periods of greater than one week (or more time than generally necessary to assess roles' functionalities). Moreover, we are pleased that CUNY officials indicate that they have taken several measures to strengthen controls over this process.
7. We acknowledge that functionality and role delegations are sometimes needed to maintain the workflows necessary for effective program and administrative operations. However, such delegations should exist for relatively short periods of time to address unusual workflow demands, for example, when an employee is absent due to illness or vacation. Moreover, we maintain that long-term role delegations should be administered similarly to standard role assignments and subject to the normal approval processes.