Controls Provided by Public Sector Retirement Plans	Tests Performed	Results
User access is administered such that users with application development roles do not have the ability to migrate application changes into production.	Inspected system generated listings of users with access to migrate application changes into production and users with development access to determine whether users with access to migrate application changes into production do not also have development access. Inspected system generated listings of users with access to production to determine that users were appropriate based on job description.	Exception noted. Testing identified one (1) developer from the population of IT promoters, with the ability to promote code changes in the UrbanCode Deployment application.
Management Response: Promoter privileges granted to the user in question were removed on August 24, 2017. Management has validated that access to the development environment for the ID in question is appropriate, and commensurate with the job responsibilities of a developer. **Additional Procedures Performed by KPMG:** KPMG obtained and inspected a system generated screenshot from the UrbanCode Deployment application which displayed that inappropriate promoter access was removed from the UrbanCode Deployment application as of August 24, 2017. Additionally, KPMG obtained and inspected a system generated screenshot from the UrbanCode Deployment application which displayed that the user did not use their promoter access for the period 1/1/2017 – 8/24/2017.		
Administrative accounts are assigned to a limited number of individuals who require those rights to perform their job duties.	Inspected system-generated listings of application, operating system, and database administrators to determine whether users on the list were authorized and access was consistent with the individual's job function.	Exceptions noted. A) Testing identified that 1 of 10 PMTS administrative IDs belong to inappropriate users who have the ability to add/modify/delete users within the PMTS application. B) Testing identified that 1 of 8 DCDirect administrative IDs belong to inappropriate users who have the ability to add/modify/delete users within the DCDirect application.
A) Management Response: Administrative application access was not removed in a timely manner when the employee changed job positions. Management determined that the transferred employee did not access the PMTS application after their transfer date and the ID was revoked from the PMTS application on September 12, 2017. **Additional Procedures Performed by KPMG:** KPMG obtained and inspected the PMTS applications and determined that the employee did not log into the PMTS application past their termination date. Additionally, KPMG obtained and inspected evidence that the PMTS ID was revoked on 9/12/2017. **B) Management Response:** Administrative application access was not removed in a timely manner when the employee changed job positions. Management determined that the transferred employee did not access the DCDirect application after their transfer date and the ID was revoked from the DCDirect application on August 31, 2017. **Additional Procedures Performed by KPMG:** KPMG obtained and inspected the DCDirect application last login date and determined that the employee did not log into the DCDirect application past their termination date. Additionally, KPMG obtained and inspected evidence that the DCDirect ID was revoked on 8/31/2017.		

Semiannually, management reviews lists of users with access to the applications to determine whether access is limited to authorized individuals and is consistent with the individual's job function.	Inspected a selection of application user access reviews to determine whether management reviewed the list of users with access to the applications on a semiannual basis. Inspected system generated evidence to determine that changes to access permissions noted by management were implemented.	Exception Noted. A. Testing identified that 7 out of 40 users marked for access permission changes by management were not implemented appropriately from the DCDirect and Taxport application. B. Out of 380 reviewers, 15 were randomly selected. Testing identified 11 of the 15 reviewers sampled did not have the adequate information to thoroughly perform the second quarter IIQ review.
A. Management Response: The DCDirect application access for all ID's was revoked on November 15, 2017. The Taxport application access for all IDs was revoked on December 5, 2017. **Additional Procedures Performed by KPMG:** KPMG obtained and inspected evidence that the DCDirect ID's were revoked on November 15, 2017 and the Taxport IDs was revoked on December 5, 2017. **B. Management Response:** All reviewers completed the required review. It was identified that additional support and training is needed to ensure adequate information is provided to the reviewers via the IIQ tool to address this issue going forward. Actions being implemented to improve the review process include updating role definitions that are viewable to the reviewer, conducting comprehensive training for all reviewers and assessing the potential realignment of the review owners.		