City of Philadelphia Pennsylvania

Office of the Controller

Assessment and Evaluation of
The City of Philadelphia's
Financial Systems Information Technology
General Controls
Fiscal Year 2025

City Controller

Christy Brady, CPA

Ensuring transparency, accountability, and fiscal integrity in city government

CITY OF PHILADELPHIA

OFFICE OF THE CONTROLLER
1230 Municipal Services Building
1401 John F. Kennedy Boulevard
Philadelphia, PA 19102-1679
(215) 686-6680 FAX (215) 686-3832

CHRISTY BRADY
City Controller

CHARLES EDACHERIL
Deputy City Controller

May 14, 2026

Mr. Rob Dubow, Director of Finance
Office of the Director of Finance
Municipal Services Building, Room
Philadelphia, PA 19102

Dear Mr. Dubow:

As part of our audit of the City of Philadelphia, Pennsylvania's (city's) Annual Comprehensive Financial Report for the fiscal year ended June 30, 2025, the Office of the Controller engaged a consultant, Eisner Advisory Group, LLC (EisnerAmper) to perform an assessment of information technology (IT) general controls for selected financial systems.

Attached are the executive summary and EisnerAmper's report detailing the results of the IT controls assessment. The findings and recommendations in the report were discussed with management. We have included management's written response to the findings and recommendations. We believe that, if implemented by management, the recommendations will improve the controls over the city's IT systems.

We would like to express our thanks to you and your staff for the courtesy and cooperation displayed during the conduct of our work.

Respectfully submitted,

Christy Brady

CHRISTY BRADY, CPA
City Controller

cc: Honorable Cherelle Parker, Mayor
Kenyatta Johnson, President, City Council
Honorable Members of City Council
Tiffany Thurman, Chief of Staff, Office of the Mayor
Members of the Mayor's Cabinet
Catherine Lamb, First Deputy Director of Finance, Finance Office
Alyssa Arjun, Deputy Director of Internal Controls and Compliance, Finance Office
Christopher Kennedy, Chief Accounting Officer, Finance Office
Melissa Scott, Chief Information Officer, Office of Innovation and Technology
Kathleen McColgan, Revenue Commissioner, Department of Revenue
Ronald Hovey, Procurement Commissioner, Procurement Department

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

EXECUTIVE SUMMARY

Why the Controller's Office Conducted the Assessment

Pursuant to the Philadelphia Home Rule Charter, the Office of the City Controller engaged Eisner Advisory Group, LLC (EisnerAmper) to conduct an assessment of the Information Technology (IT) general controls for selected financial systems. The objective of this assessment was to evaluate the IT controls over key financial-related applications in connection with the Controller's Office audit of the City of Philadelphia, Pennsylvania's Annual Comprehensive Financial Report for the fiscal year ended June 30, 2025.

What the Controller's Office Found

Key findings in the report are listed below. We believe these findings and others described in the report warrant the attention of management.

- With regard to periodic user access reviews (UARs), exceptions were identified in the documentation and execution of UARs in ACIS, and a UAR was not performed at all for PHLContracts and the Office of Innovation and Technology (OIT).
- Concerning ACIS, exceptions were identified related to documentation and segregation of duties between development, test, and production environments. Specifically, five out of five change management requests were not fully documented, individuals with system administrator access had the ability to both develop changes in the development environment and migrate those changes into the production environment, and there was no post change monitoring control in place.
- Regarding PHLContracts, there was a lack of documentation and operation of logical access controls. Testing revealed privileged access provisioning was not adequately documented, and termination controls were not operating effectively.

What the Controller's Office Recommends

The Controller's Office has developed a number of recommendations to address the findings noted above. These recommendations can be found in the body of the report.

Assessment and Evaluation of IT General Controls

EISNERAMPER

Eisner Advisory Group LLC
One Logan Square
130 North 18th Street, Suite 3000
Philadelphia, PA 19103
T 215.881.8800
F 215.881.8801
www.eisneramper.com

Hon. Christy Brady
City Controller
City of Philadelphia
1401 JFK Boulevard, 12th Floor
Philadelphia, Pennsylvania 19102

We have concluded our engagement to perform an evaluation of the information technology general controls supporting key financial systems of the City of Philadelphia. This engagement was agreed to by the City of Philadelphia – Office of the Controller (the Controller's Office) and was performed solely to assist in evaluating the IT general controls in connection with the Controller's Office audit of the City of Philadelphia's fiscal year 2025 Annual Comprehensive Financial Report (ACFR).

Management of the City of Philadelphia is responsible for the operations of internal controls over, the City's information technology environment. The sufficiency of the scope and procedures of our engagement is solely the responsibility of the management of the Controller's Office. Consequently, we make no representations regarding the sufficiency of the scope and procedures described in the attached document either for the purpose for which this report has been requested or for any other purpose.

The engagement was performed in accordance with applicable professional standards, including the Statements on Standards for Consulting Services issued by the American Institute of Certified Public Accountants (AICPA). EisnerAmper did not perform an audit, review, or compilation in accordance with Generally Accepted Government Auditing Standards or with attest standards established by the AICPA.

The procedures performed were limited to those described herein based on documentation provided, interviews and process walkthroughs with City personnel, and other information obtained, including whether IT general controls were placed in operation and adequately designed as of June 30, 2025. Information obtained subsequent to the date of this report may affect this analysis. The procedures were performed solely with respect to the above-referenced engagement. This report is not to be reproduced, distributed, disclosed, or used for any other purpose.

We have attached observations and recommendations regarding IT general controls resulting from this consulting engagement for the consideration of the Controller's Office. Our procedures focused on IT general controls over security management, access controls, segregation of duties, configuration management, and contingency planning. The results of our procedures identified deficiencies related to IT general controls. No material weaknesses were identified.

The procedures performed and related observations and recommendations are described in the attached document. We performed our procedures during the months of October 2025 through February 2026.

Sincerely,

Eisner Advisory Group, LLC

Eisner Advisory Group, LLC.
March 27, 2026

City of Philadelphia – Office of the Controller
Assessment and Evaluation of the City of Philadelphia's In-Scope Applications
IT General Controls
As of June 30, 2025

Table of Contents

City of Philadelphia – Office of the Controller
Assessment and Evaluation of the City of Philadelphia's In-Scope Applications
IT General Controls
As of June 30, 2025

Executive Summary

The Controller's Office engaged Eisner Advisory Group, LLC (EisnerAmper), to perform an assessment of Information Technology (IT) general controls supporting key financial systems of the City of Philadelphia.

This engagement was conducted in accordance with the Statements on Standards for Consulting Services issued by the American Institute of Certified Public Accountants (AICPA). The scope of the assessment was limited to IT general controls designed and in place as of June 30, 2025. Our procedures were performed during the months of October 2025 through February 2026 and included testing the design, implementation, and operating effectiveness of selected IT general controls.

A summary of observations and their potential impact is presented below.

Summary of Objective, Scope, and Methodology

The objective of the EisnerAmper consulting engagement was to evaluate whether IT general controls were appropriately designed, implemented, and operating effectively in support of the Controller's Office audit of the City of Philadelphia's fiscal year 2025 Annual Comprehensive Financial Report (ACFR). The scope of the assessment included IT general controls in place as of June 30, 2025.

The scope of the EisnerAmper consulting engagement also included follow up on the IT general and application control deficiencies reported in the City of Philadelphia's fiscal year 2024 Report on Internal Control and Compliance.

In addition, our engagement was structured to address the following five (5) areas for the IT general controls as requested by the Controller's Office:

1. *Security Management* - the controls designed and placed into operation to provide reasonable assurance that security management is effective.

2. *Access Controls* - the controls designed and placed into operation to provide reasonable assurance that access to computer resources (data, equipment, and facilities) is reasonable and restricted to authorized individuals.

3. *Configuration Management* - the controls designed and placed into operation to provide reasonable assurance that changes to information system resources are authorized, and systems are configured and operated securely and as intended.

4. *Segregation of Duties* - the controls designed and placed into operation to provide reasonable assurance that incompatible duties are effectively segregated.

5. *Contingency Planning* - the controls designed and placed into operation to provide reasonable assurance that contingency planning (1) protects information resources and minimizes the risk of unplanned interruptions and (2) provides for recovery of critical operations should interruptions occur.

City of Philadelphia – Office of the Controller
Assessment and Evaluation of the City of Philadelphia's In-Scope Applications
IT General Controls
As of June 30, 2025

Summary of Observations

Below is a summary of key observations identified through the procedures performed during this engagement. Based on the potential impact on the City of Philadelphia's fiscal year 2025 ACFR, each observation was assigned a rating. [1] Additional details supporting these observations are provided in the detailed sections of this report.

Application	Findings	Potential Impact
ACIS	Inadequate Change Management Documentation and Segregation of Duties	Significant Deficiency
	Inadequate Documentation and Evidence Supporting User Access Termination and Reviews	Significant Deficiency
PHLContracts	Inadequate Documentation and Execution of Privileged Access Provisioning, Termination, and User Access Reviews (UARs)	Significant Deficiency
	Vendor-Pushed Changes Are Not Formally Approved or Acknowledged	Control Deficiency
	Inadequate Review of SOC 1 Report	Control Deficiency
Office of Innovation and Technology	Lack of Periodic UARs	Significant Deficiency
FAMIS & ADPICS	Lack of Segregation of Duties Between Test and Production Environments	Control Deficiency
	Untimely Removal of User Access and Missing Termination Documentation	Control Deficiency
	Lack of Periodic UARs (ADPICS)	Control Deficiency

[1] The AICPA's *Professional Standards (Clarified)* AU-C Section 265.07 states that 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. AU-C Section 265.07 provides the following definitions:
Material Weakness – This is a deficiency, or a 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.
Significant Deficiency – This is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness yet important enough to merit attention by those charged with governance.

City of Philadelphia – Office of the Controller
Assessment and Evaluation of the City of Philadelphia's In-Scope Applications
IT General Controls
As of June 30, 2025

Application	Findings	Potential Impact
	Inadequate Documentation Supporting UARs (FAMIS)	Control Deficiency
Basis2	Lack of Testing and Approvals Prior to Deployment	Control Deficiency
	Unrevoked Access for Terminated Employees and Consultants	Control Deficiency
	Lack of Periodic UARs	Control Deficiency
OnePhilly	Inadequate UAR Process	Control Deficiency
	Inadequate Review of SOC 1 Report	Control Deficiency
PRISM	Inadequate Documentation and Segregation of Duties for Production Migrations	Control Deficiency
	Lack of Executive Approval for Emergency Application Changes	Control Deficiency
	Inadequate UAR Process	Control Deficiency
	Inadequate Review of SOC 1 Report	Control Deficiency

City of Philadelphia – Office of the Controller
Assessment and Evaluation of the City of Philadelphia's In-Scope Applications
IT General Controls
As of June 30, 2025

Our engagement was structured to address the five (5) areas for IT general controls. Within each area, we focused on several control elements as follows:

Security Management	• A Security management program is in place
	• Periodic assessments and validation of risk
	• Security control policies and procedures
	• Security awareness training and other security related personnel issues
	• Periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices
	• Remediation of information security weaknesses
	• Security over activities performed by external third parties
Access Controls	• Protection of information system boundaries
	• Identification and authentication mechanisms
	• Authorization controls
	• Protection of sensitive system resources
	• Audit and monitoring capability, including incident handling
	• Physical security controls
Configuration Management	• Configuration management policies, plans, and procedures
	• Current configuration identification information
	• Proper authorization, testing, approval, and tracking of all configuration changes
	• Routine monitoring of the configuration
	• Updating software on a timely basis to protect against known vulnerabilities
	• Documentation and approval of emergency changes to the configuration
Segregation of Duties	• Segregation of incompatible duties and responsibilities and related policies
	• Control of personnel activities through formal operating procedures, supervision, and review
Contingency Planning	• Protection of information resources and minimizing the risk of unplanned interruptions
	• Provision for recovery of critical operations should interruptions occur, including effective: o Assessment of the criticality and sensitivity of computerized operations and identification of supporting resources; o Steps taken to prevent and minimize potential damage and interruption; o Comprehensive contingency plan; and o Periodic testing of the contingency plan, with appropriate adjustments to the plan based on testing.

Detailed Results

Observations

Below is our summary and the supporting detail for the observations noted through the procedures performed for this engagement. Our observations include the details of the condition, the criteria, the potential cause, the effect, and our recommendation.

ACIS

1. Inadequate Change Management Documentation and Segregation of Duties

Potential Impact: **Significant Deficiency**

Condition: Although change management controls exist within the ACIS application, exceptions were identified related to documentation and segregation of duties between Development, Test, and Production environments, specifically:

- Five out of five change management requests were not fully documented, as supporting evidence such as testing results, management approval, and identification of the individual responsible for migrating changes to production was incomplete or not retained.
- Individuals with ACIS System Administrator access had the ability to both develop changes in the development environment and migrate those changes into the production environment.
- There was no post change monitoring control in place to confirm that users were not promoting their own changes into production, resulting in inadequate segregation of duties.

Criteria: Effective change management controls require that all system changes be formally documented, tested, approved, and migrated to production by authorized individuals who are independent of the change developer. Documentation should clearly identify evidence of testing, approvals, and the individual responsible for migrating changes to production to demonstrate appropriate segregation of duties and management oversight.

Potential Cause: Management has not consistently enforced documentation requirements for change management activities and has not implemented controls to ensure segregation of duties between individuals developing changes and those migrating changes into production.

Effect: Without complete documentation and adequate segregation of duties, there is an increased risk that unauthorized, untested, or inappropriate changes may be introduced into the production environment. This could adversely affect system functionality, data integrity, or security and limit management's ability to effectively monitor and review change activities.

Recommendation: Management should ensure that all change management requests are fully documented, including evidence of testing, management approval, and identification of the individual who migrated the change to production. In addition, management should implement controls to

enforce segregation of duties between development and production migration activities, including preventing users from promoting their own changes into production.

2. Inadequate Documentation and Evidence Supporting User Access Termination and Access Reviews

Potential Impact: **Significant Deficiency**

Condition: Exceptions were identified in the documentation and execution of user access termination and periodic User Access Review (UAR) activities within ACIS, specifically:

- Although the users were inactive at the time of testing, documentation supporting the timely removal of access for five out of five sample terminated users was not consistently maintained.
- For two of five samples, supporting documentation, such as payroll termination notices or corresponding access removal requests, was not consistently retained.
- For five of five sampled departments, evidence supporting the completion of the periodic UAR was insufficient. Responses documenting approval from the reviewer and requested access changes (if any) was not provided.
- The population used for the UAR was manually compiled and lacked documented procedures to validate completeness. Additionally, system-generated listings used during testing did not align with the review period.

Criteria: OIT's Access Control Policy requires that user access be promptly removed upon termination and that periodic UARs be well documented and performed using a complete and accurate population of users. These activities should be supported by documented evidence, including approval signoffs, access removal requests, and validation of population completeness, to demonstrate effective oversight and compliance with access management requirements.

Potential Cause: Management has not formalized or consistently enforced procedures for documenting user access termination activities or for compiling, validating, and evidencing the completion of periodic UARs.

Effect: Without sufficient documentation and evidence supporting user access termination and access review activities, there is an increased risk that terminated users may retain access longer than appropriate or that inappropriate access may not be identified and remediated in a timely manner. This increases the risk of unauthorized access and may adversely affect system security and data integrity.

Recommendation: Management should formalize and document procedures for user access termination to ensure timely removal of access and retention of supporting documentation. Additionally, management should document the methodology used to compile and validate the completeness of the user population used as part of the user access review, retain evidence of reviewer approval, and document all access changes resulting from the review.

PHLContracts

3. Inadequate Documentation and Execution of Privileged Access Provisioning, Termination, and User Access Reviews

Potential Impact: **Significant Deficiency**

Condition: Exceptions were identified in the documentation and operation of logical access controls within the PHLContracts application, specifically:

- Privileged access provisioning was not adequately documented, as evidence supporting management approval and business justification for privileged access was not consistently maintained.
- Termination controls were not operating effectively. Documentation evidencing timely access removal for two sampled terminated users was not consistently retained. Additionally, thirteen terminated users were identified as retaining PHLContracts access at the time of testing.
- A periodic UAR was not performed for PHLContracts. Reviews of standard and privileged users, associated permissions, and incompatible access combinations were not conducted.

Criteria: OIT's Access Control Policy requires that privileged access be formally approved and documented, user access be promptly removed upon termination, and periodic UARs be performed to validate that access remains appropriate. These activities should be supported by retained documentation demonstrating management approval, timely execution, and effective oversight.

Potential Cause: Management has not established or consistently enforced formal procedures for documenting privileged access provisioning, executing, and evidencing timely access removal upon termination, or performing periodic UARs within the PHLContracts application.

Effect: Without adequate documentation and execution of access provisioning, termination, and review controls, there is an increased risk that users may retain inappropriate or excessive access. This could result in unauthorized access to the application, increased fraud risk, or violations of segregation of duties principles.

Recommendation: Management should formalize and document procedures for privileged access provisioning, including retention of approval and business justification. In addition, management should strengthen termination controls to ensure timely access removal and retention of supporting documentation. Finally, management should implement a periodic UAR process that includes review of all access, evaluation of roles and associated permissions, and identification of incompatible role assignments to determine that the access is still considered appropriate. The review should be formally documented, include evidence of the completeness and accuracy of procedures performed, reviewer approval, and capture any access changes or remediation actions resulting from the review.

4. Vendor-Pushed Changes Are Not Formally Approved or Acknowledged

Potential Impact: **Deficiency**

Condition: PHLContracts application changes are submitted to and implemented by the vendor; however, management was unable to demonstrate procedures to ensure the completeness and accuracy of change management population as well as to evidence post-implementation verification and acknowledgement that changes were successfully implemented by the vendor as intended.

Criteria: Effective change management controls require that system changes, including vendor-implemented changes, be formally reviewed, approved, and subject to post-implementation verification. Management should maintain documentation evidencing approval, acknowledgment, and validation of changes to ensure changes are authorized and implemented as intended.

Potential Cause: Management has not established formal processes to approve, acknowledge, or document vendor-pushed changes or to perform post-implementation verification of changes within the PHLContracts application.

Effect: Without formal approval and verification of vendor-implemented changes, there is an increased risk that unauthorized or inappropriate changes could be introduced into the application. This may adversely affect system functionality, data integrity, or security and limits management's ability to effectively oversee change activities.

Recommendation: Management should establish procedures to obtain a complete population of changes from the system when required, formally approve or acknowledge vendor-pushed changes, and perform post-implementation verification to confirm changes were implemented successfully. Supporting documentation should be retained to demonstrate management oversight of change management activities.

5. Inadequate Review of SOC 1 Report

Potential Impact: **Deficiency**

Condition: The City did not perform a comprehensive, documented review of the Periscope SOC 1 report during the audit period. Specifically, documentation evidencing evaluation of the SOC report, including whether the opinion was qualified or unqualified and the relevance of complementary user entity controls, was not maintained.

Criteria: Management should perform and document a periodic review of SOC reports for third-party service providers. This review should include evaluation of the auditor's opinion, identification of relevant control objectives, and identification of complementary user entity controls to ensure reliance on the service organization is appropriate.

Potential Cause: Management has not formalized procedures for reviewing and documenting SOC reports related to third-party systems supporting the PHLContracts application.

Effect: Without a documented SOC report review, management may not identify control gaps, qualified opinions, or required complementary user entity controls. This increases the risk that deficiencies at the service organization could adversely impact system operations, data integrity, or security.

Recommendation: Management should establish and document procedures for reviewing SOC reports, including evaluation of the auditor's opinion and exceptions (if any), identification of relevant complementary user entity controls and if applicable obtain associated bridge letters. Evidence of the review should be retained to demonstrate management oversight and support reliance on third-party service providers.

Office of Innovation and Technology (OIT)

6. Lack of Periodic User Access Reviews

Potential Impact: **Significant Deficiency**

Condition: During the audit period, OIT did not perform a review of standard and privileged user access. Specifically, the UAR process was ineffective due to the following:

- A review of standard and privileged users was not performed.
- A review of user roles and associated permissions was not performed.
- A review of incompatible roles assigned to users was not performed.

As a result, there was no evidence to demonstrate that user access within OIT-managed systems was periodically reviewed for appropriateness or segregation of duties conflicts.

Criteria: OIT's Access Control Policy requires management to perform periodic, documented UARs to ensure that standard and privileged access remains appropriate. These reviews should include evaluation of user roles, associated permissions, and identification of incompatible role assignments to support effective segregation of duties and compliance with access management requirements.

Potential Cause: Management has not established or consistently enforced formal procedures for performing and documenting periodic UARs, including role and segregation-of-duties analysis.

Effect: Without a documented and periodically performed UAR, users may retain inappropriate or excessive access, including incompatible role combinations. This increases the risk of unauthorized access, inappropriate system activity, or violations of segregation of duties principles, which could adversely affect system security and data integrity.

Recommendation: Management should implement a periodic UAR process that includes review of standard and privileged users, evaluation of roles and associated permissions, and identification of incompatible role assignments to determine that the access is still considered appropriate. The review should be formally documented, include evidence of the completeness and accuracy of procedures performed, reviewer approval, and capture any access changes or remediation actions resulting from the review.

FAMIS & ADPICS

7. Lack of Segregation of Duties Between Test and Production Environments

Potential Impact: **Deficiency**

Condition: Segregation of duties between the test and production environments within the FAMIS and ADPICS applications was not adequately enforced. Specifically:

- System-enforced restrictions to prevent users from promoting their own changes into production were not implemented.
- There was no monitoring control in place to detect or prevent changes being migrated to production by unauthorized individuals.

Criteria: Effective change management controls require segregation of duties between individuals developing or testing changes and those migrating changes into the production environment. Monitoring controls should be in place to detect unauthorized changes, and documentation should support management review and oversight of production migrations.

Potential Cause: Management has not implemented system-enforced or compensating controls to restrict or monitor user activity between test and production environments, nor has documentation standards been consistently enforced.

Effect: Without adequate segregation of duties and monitoring controls, there is an increased risk that unauthorized or inappropriate changes may be migrated into production. This could adversely affect system functionality, data integrity, or security.

Recommendation: Management should implement controls to enforce segregation of duties between test and production environments, including restricting users from promoting their own changes. In addition, management should establish monitoring and documentation requirements to ensure production migrations are reviewed, approved, and performed by authorized individuals.

8. Untimely Removal of User Access and Missing Termination Documentation

Potential Impact: **Deficiency**

Condition: User access to the FAMIS and ADPICS applications was not consistently removed in a timely manner following documented termination dates. Specifically:

- Documentation supporting the termination of user access was not consistently retained.
- Termination request documentation was not available for review.
- Instances were identified where terminated users remained active or retained access beyond their termination date.

Although all users sampled were inactive at the time of testing, the timeliness of deprovisioning and adherence to documented termination procedures could not be validated.

Criteria: OIT's Access Control Policy requires that user access be promptly removed upon termination and that supporting documentation be retained to evidence timely deprovisioning and management oversight.

Potential Cause: Management has not consistently enforced termination procedures or documentation retention requirements for access removal within the FAMIS and ADPICS applications.

Effect: Without timely removal of access and supporting documentation, there is an increased risk that terminated users may retain access longer than appropriate. This increases the risk of unauthorized access and may adversely affect system security.

Recommendation: Management should redesign termination controls and communicate to the associated stakeholders the updated process to ensure user access is removed promptly upon termination and that documentation evidencing approval and completion of access removal is retained in accordance with access management policies.

9. Lack of Periodic User Access Reviews (ADPICS)

Potential Impact: **Deficiency**

Condition: A periodic UAR was not performed for the ADPICS application during the audit period, specifically:

- A review of standard and privileged users was not conducted.
- A review of user roles and associated permissions was not performed.
- A review of incompatible roles assigned to users was not performed.

As a result, there was no evidence to demonstrate that user access was periodically reviewed for appropriateness or segregation of duties conflicts.

Criteria: OIT's Access Control Policy requires management to perform periodic, documented UARs to ensure that standard and privileged access remains appropriate. These reviews should include evaluation of user roles, associated permissions, and identification of incompatible role assignments to support effective segregation of duties and compliance with access management requirements.

Potential Cause: Management has not established or consistently enforced formal procedures for performing and documenting periodic UARs, including role and segregation of duties analysis within the ADPICS application.

Effect: Without a documented and periodically performed UAR, users may retain inappropriate or excessive access, including incompatible role combinations. This increases the risk of unauthorized access, inappropriate system activity, or violations of segregation of duties principles, which could adversely affect system security and data integrity.

Recommendation: Management should implement a periodic UAR process for ADPICS that includes review of standard and privileged users, evaluation of roles and associated permissions, and identification of incompatible role assignments to determine that the access is still considered appropriate. The review should be formally documented, include evidence of the completeness and accuracy of procedures performed, reviewer approval, and capture any access changes or remediation actions resulting from the review.

10. Inadequate Documentation Supporting User Access Reviews (FAMIS)

Potential Impact: **Deficiency**

Condition: Documentation supporting the periodic UAR for the FAMIS application was not adequately retained, specifically:

- User listings provided did not reference the department responsible for validating completeness or include documentation evidencing management validation of the population.
- The population reviewed and the approval and implementation of access changes could not be validated.
- Responsibilities for role assignments, role-permission mapping, and analysis of incompatible or conflicting access combinations were not clearly documented.

Criteria: OIT's Access Control Policy requires UARs to be supported by complete and retained documentation, including evidence of population completeness, reviewer approval, and analysis of roles and permissions. Documentation should clearly demonstrate that access reviews were performed in accordance with management expectations.

Potential Cause: Management has not consistently enforced formal procedures for performing and documenting periodic UARs, including role and segregation of duties analysis within the ADPICS application.

Effect: Without sufficient documentation supporting UARs, management cannot demonstrate that access was reviewed for appropriateness or that identified issues were remediated. This increases the risk of unauthorized access, inappropriate system activity, or violations of segregation of duties principles, which could adversely affect system security and data integrity.

Recommendation: Management should formalize documentation requirements for UARs, including a review of all users, evaluation of roles and associated permissions, and identification of incompatible role assignments to determine that the access is still considered appropriate. The review should be formally documented, include evidence of the completeness and accuracy of procedures performed, reviewer approval, and capture any access changes or remediation actions resulting from the review.

Basis2

11. Lack of Testing and Approvals Prior to Deployment

Potential Impact: **Deficiency**

Condition: Documentation supporting production migration activities for the Basis2 application was not consistently maintained to demonstrate that changes were tested and approved prior to deployment, specifically:

- For one sample, approvals prior to deployment were not available.
- For another sample, the testing and approval were obtained post deployment. Pre-change testing or approval evidence were also unavailable.

As a result, it could not be demonstrated that all changes were appropriately tested and formally approved prior to being migrated to production.

Criteria: Effective change management controls require that system changes be formally documented, tested, and approved prior to migration to the production environment. Documentation should evidence testing results, management approval, and compliance with established change management policies.

Potential Cause: Management has not consistently enforced documentation and evidence retention requirements for production migrations within the Basis2 change management process.

Effect: Without complete documentation supporting production migrations, there is an increased risk that unauthorized, untested, or inappropriate changes may be migrated into production. This could adversely impact system functionality, data integrity, or security.

Recommendation: Management should ensure that all production migrations are supported by complete documentation, including evidence of pre-implementation testing and management approval. Documentation should be retained in accordance with change management policies to demonstrate effective oversight.

12. Unrevoked Access for Terminated Employees and Consultants

Potential Impact: **Deficiency**

Condition: User access for terminated employees and consultants within the Basis2 application was not consistently revoked in a timely manner, specifically:

- For two of three samples tested, access termination procedures were performed manually against names with spelling variations, as such, access was not removed in a timely manner.
- For one of three samples, user termination was not communicated to the Basis2 team, resulting in continued system access at the time of testing.

Criteria: OIT's Access Control Policy requires that user access be promptly removed upon termination and that termination processes be supported by accurate, complete, and timely communication from authoritative sources, such as HR systems.

Potential Cause: Management relies on a manual termination process that is not integrated or a match with HR data and does not consistently ensure timely communication of termination events to system administrators.

Effect: Without timely revocation of access for terminated users, there is an increased risk that former employees or consultants may retain inappropriate access to the system. This increases the risk of unauthorized access and potential misuse of system data.

Recommendation: Management should strengthen termination controls by implementing procedures to address potential spelling differences to ensure timely notification of terminations, and prompt removal of system access. Where feasible, termination processes should be automated or integrated with HR systems to reduce reliance on manual processes.

13. Lack of Periodic User Access Reviews

Potential Impact: **Deficiency**

Condition: A periodic UAR was not performed for the Basis2 application during the audit period, specifically:

- A review of standard and privileged users was not performed.
- A review of user roles and associated permissions was not conducted.
- A review of incompatible roles assigned to users was not performed.

As a result, there was no evidence to demonstrate that user access was periodically reviewed for appropriateness or segregation of duties conflicts.

Criteria: OIT's Access Control Policy requires management to perform periodic, documented UARs to ensure that standard and privileged access remains appropriate. These reviews should include evaluation of user roles, associated permissions, and identification of incompatible role assignments to support effective segregation of duties and compliance with access management requirements.

Potential Cause: Management has not established or consistently enforced formal procedures for performing and documenting periodic UARs including role and segregation of duties analysis within the Basis2 application.

Effect: Without a documented and periodically performed UAR, users may retain inappropriate or excessive access, including incompatible role combinations. This increases the risk of unauthorized access, inappropriate system activity, or violations of segregation of duties principles, which could adversely affect system security and data integrity.

Recommendation: Management should implement a periodic UAR process for Basis2 that includes review of standard and privileged users, evaluation of roles and associated permissions, and identification of incompatible role assignments to determine that the access is still considered appropriate. The review should be formally documented, include evidence of the completeness and accuracy of procedures performed, reviewer approval, and capture any access changes or remediation actions resulting from the review.

OnePhilly

14. Inadequate User Access Review Process

Potential Impact: **Deficiency**

Condition: The UAR process for the OnePhilly application was not effectively designed or operating during the audit period, specifically:

- The UAR process does not mandate a response from reviewers.
- There was no evidence demonstrating the completeness and accuracy of the UAR listing.
- There was no evidence that access modifications identified during the review were completed in a timely manner.

As a result, management could not demonstrate that user access remained appropriate or aligned with users' current job responsibilities. Additionally, the segregation of duties policy was not reviewed during the audit period, and a segregation of duties roles matrix was not provided.

Criteria: OIT's Access Control Policy requires a documented and periodically performed UAR process to ensure that standard and privileged access remains appropriate. The review should include a complete and accurate population of users, assignment of appropriate reviewers, required reviewer responses, and documentation of timely remediation of identified access changes.

Potential Cause: Management does not have the ability to enforce a formalized UAR process that requires a documented response. Additionally, a process has not been established to define reviewer responsibilities, document population completeness validation, or follow-up requirements.

Effect: Without an effective UAR process, users may retain inappropriate or excessive access, increasing the risk of unauthorized access or activities that could adversely affect system security and data integrity.

Recommendation: Management should formalize and implement a UAR process for OnePhilly that mandates reviewer responses, documents the completeness and accuracy of the user population, and ensures timely completion and documentation of access modifications resulting from the review. Additionally, management should review and approve the segregation of duties policy and roles matrix annually, every fiscal year.

15. Inadequate Review of SOC 1 Report

Potential Impact: **Deficiency**

Condition: The City did not perform a comprehensive, documented review of the Oracle EBS SOC 1 report during the audit period. Specifically, documentation evidencing management's evaluation of the SOC report, including whether the auditor's opinion was qualified or unqualified, and identification of relevant complementary user entity controls was not maintained.

Criteria: Management should perform and document a periodic review of SOC reports for third-party service providers. This review should include evaluation of the auditor's opinion, assessment of relevant control objectives, and identification of complementary user entity controls to support reliance on the service organization.

Potential Cause: Management has not formalized procedures for reviewing and documenting SOC reports related to third-party systems supporting the OnePhilly application.

Effect: Without a documented SOC report review, management may not identify control deficiencies, qualified opinions, or required complementary user entity controls. This increases the risk that deficiencies at the service organization could adversely impact system operations, data integrity, or security.

Recommendation: Management should establish and document procedures for reviewing SOC reports, including evaluation of the auditor's opinion and exceptions (if any), identification of relevant complementary user entity controls and if applicable obtain associated bridge letters. Evidence of the review should be retained to demonstrate management oversight and support reliance on third-party service providers.

PRISM

16. Inadequate Documentation and Segregation of Duties for Production Migrations

Potential Impact: **Deficiency**

Condition: Documentation supporting production migration activities within the PRISM application was not consistently maintained, and segregation of duties was not adequately enforced. Specifically:

- For one sample tested, the change was developed, tested, and deployed by the same individual, demonstrating no evidence of segregation of duties for this change.
- No monitoring control was in place to perform a review or independently validate changes migrated to production post deployment.

Criteria: Effective change management controls require that production migrations be performed by authorized individuals who are independent of the change developer. In addition, documentation and monitoring controls should be in place to evidence management oversight and compliance with segregation of duties requirements.

Potential Cause: Management has not consistently enforced segregation of duties requirements or implemented monitoring controls to independently review production migrations within the PRISM application.

Effect: Without adequate segregation of duties and monitoring of production migrations, there is an increased risk that unauthorized or inappropriate changes may be introduced into the production environment. This could adversely affect system functionality, data integrity, or security.

Recommendation: Management should enforce segregation of duties controls to ensure individuals developing or testing changes cannot migrate those changes to production. In addition, management should implement monitoring controls and retain documentation, evidencing independent review of production migrations.

17. Lack of Executive Approval for Emergency Application Changes

Potential Impact: **Deficiency**

Condition: For each of the five samples tested, emergency change management documentation for changes made to the PRISM application did not consistently evidence executive stakeholder approval as required by the PRISM change management policy.

Criteria: Change management policies require that emergency application changes be formally approved by appropriate stakeholders, including executive management, prior to implementation. Documentation should evidence such approvals to demonstrate compliance with policy and management oversight.

Potential Cause: Management has not consistently enforced change management policy requirements related to obtaining and documenting executive approval for emergency application changes.

Effect: Without documented executive approval, emergency changes may be implemented without appropriate oversight or alignment with management expectations. This increases the risk of unauthorized or inappropriate changes impacting system operations or data integrity.

Recommendation: Management should ensure that all emergency application changes are supported by documented executive approval in accordance with the change management policy. Change tickets should be updated to require and retain evidence of such approvals prior to implementation.

18. Inadequate User Access Review Process

Potential Impact: **Deficiency**

Condition: The UAR process for the PRISM application was not effectively designed or operating during the audit period, specifically:

- Documentation supporting periodic UARs was not retained.
- User listings were not returned by departments, preventing validation of the completeness and accuracy of the population reviewed.
- Evidence supporting review and approval of access changes was not available.
- The appropriateness of roles assigned relative to job responsibilities and evaluation of role-to-permission mappings, including analysis of incompatible or conflicting access combinations, could not be validated.

Criteria: OIT's Access Control Policy require periodic, documented UARs to ensure that standard and privileged access remains appropriate. These reviews should be supported by complete and accurate user populations, include evaluation of user roles, associated permissions, and identification of incompatible role assignments to support effective segregation of duties and compliance with access management requirements.

Potential Cause: Management has not formalized or consistently enforced procedures for performing, documenting, and retaining evidence of periodic UARs within the PRISM application.

Effect: Without an effective UAR process, users may retain inappropriate or excessive access, increasing the risk of unauthorized access or segregation of duties violations that could adversely affect system security and data integrity.

Recommendation: Management should formalize and implement a periodic UAR process for PRISM that includes documented validation of population completeness, review of standard and privileged users, evaluation of roles and associated permissions, and identification of incompatible role assignments. The review should be formally documented, include evidence of reviewer approval, and capture any access changes or remediation actions resulting from the review.

19. Inadequate Review of SOC 1 Report

Potential Impact: **Deficiency**

Condition: The City did not perform a comprehensive, documented review of the Fast Holding Services LLC SOC 1 report during the audit period. Specifically, documentation evidencing management's evaluation of the SOC report, including whether the auditor's opinion was qualified or unqualified, and identification of relevant complementary user entity controls was not maintained.

Criteria: Management should perform and document periodic reviews of SOC reports for third-party service providers. This review should include evaluation of the auditor's opinion, assessment of relevant control objectives, and identification of complementary user entity controls to support reliance on the service organization.

Potential Cause: Management has not formalized procedures for reviewing and documenting SOC reports related to third-party service providers supporting the PRISM application.

Effect: Without a documented SOC report review, management may not identify control deficiencies, qualified opinions, or required complementary user entity controls. This increases the risk that deficiencies at the service organization could adversely impact system operations, data integrity, or security.

Recommendation: Management should establish and document procedures for reviewing SOC reports, including evaluation of the auditor's opinion and exceptions (if any), identification of relevant complementary user entity controls and if applicable obtain associated bridge letters. Evidence of the review should be retained to demonstrate management oversight and support reliance on third-party service providers.

Remediation Status of Prior Reported Findings

As part of this engagement, EisnerAmper followed up on the remediation status of IT general control weaknesses noted by the Controller's Office in the City fiscal year 2024 Report on Internal Control and Compliance. For the eight (8) previously reported findings we noted three (3) as remediated, four (4) as partially remediated and one (1) as not remediated. These remediated conditions included the following items:

IT General Controls

2024-003: OIT's Access Controls and Segregation of Duties for Key Financial Systems Still Require Strengthening

Prior Condition: Weaknesses persisted in OIT's general IT controls, including lack of documented user access reviews, inconsistent onboarding and offboarding documentation, and unapproved policies.

Remediation Status: **Partially Remediated** - During the current assessment, we confirmed that a review of standard and privileged users did not occur during the audit period. Additionally, we confirmed the process for granting new system access, revoking access for employee terminations or departures, and of OnePhilly notifying OIT of terminations has been formally documented. As a result, this finding is considered partially remediated, refer to 2025 Finding #6.

2024-004: ACIS' User Access Controls Still Require Strengthening

Prior Condition: The Procurement Department did not perform user access reviews (UARs) for ACIS and allowed users to maintain both executive and administrator access without documented approval or exemption.

Remediation Status: **Partially Remediated** - During the current assessment, we noted that sufficient evidence to support completion of an application-specific UAR was not provided. Evidence supporting a completed UAR remained pending at the time of testing. It was confirmed a Risk Acceptance form for non-IT users with executive and administrator access to ACIS was completed and approved to justify the users' continued access needs. As a result, this finding is considered partially remediated, refer to 2025 Finding #2.

2024-005: PRISM's User Access Approvals Were Not Documented, and Periodic User Access Review Was Not Performed

Prior Condition: The PRISM team lacked documentation supporting new user authorizations, did not perform periodic user access reviews, and allowed separated users to retain access for extended periods.

Remediation Status: **Partially Remediated** - During the current assessment, it was noted that tickets were used and approved for both onboarding and offboarding access requests, and screenshots of the monthly "User Access Summary" generated within the PRISM system were obtained. However, additional evidence supporting review, approval, and access modification procedures used to complete the UAR remained

pending. As a periodic UAR was not fully performed or evidenced, this finding is considered partially remediated, refer to 2025 Finding #18.

2024-006: OnePhilly System's Access Controls Need Improvement

Prior Condition: The OnePhilly team did not provide documentation supporting user access reviews, and segregation of duties was not adequately enforced for users with privileged access.

Remediation Status: **Partially Remediated** - During the current assessment, we noted that OnePhilly facilitates and documents UARs; however, the review process remains ineffective as some reviewers do not respond, as the OnePhilly team does not have the ability to modify access for groups that do not confirm access or respond to review requests. Additionally, the Segregation of Duties policy was not reviewed during the audit period, and a Segregation of Duties roles matrix was not provided. Finally, management confirmed that all users with privileged access were considered appropriate. As a result, this finding is considered partially remediated, refer to 2025 Finding #14.

2024-014: Certain Other General IT Controls for OIT Still Need Improvement

Prior Condition: OIT did not perform disaster recovery testing in fiscal year 2024 and failed to update its disaster recovery plan and change management policy.

Remediation Status: **Remediated** - During the current assessment, we confirmed that OIT conducted a disaster recovery test during the audit period. In addition, the change management standard operating procedure and the disaster recovery plan was modified to include clear documentation standards. The OIT Change Management Standard Operating Procedure was reviewed and approved and outlines documentation standards for end-user testing and approvals. Based on the procedures performed, this finding was confirmed as remediated.

2024-015: Disaster Recovery Testing Had Not Been Performed for PRISM

Prior Condition: PRISM disaster recovery testing was incomplete, leaving critical components untested.

Remediation Status: **Remediated** - During the current assessment, we confirmed that a PRISM disaster recovery test was performed during the audit period. Based on the procedures performed, this finding was confirmed as remediated.

2024-016: OnePhilly Physical Security Policy Was Still Not Reviewed

Prior Condition: OnePhilly management did not provide sufficient documentation evidencing review and approval of the Physical Security Policy.

Remediation Status: **Remediated** - During the current assessment, EisnerAmper confirmed the Physical Security policy, Access Control policy, and where the OnePhilly system is physically hosted is the responsibility of the vendor with details included in the vendor's SOC 1 type 2 report. Based on the procedures performed,

this finding was confirmed as remediated. For details on the review of the OnePhilly vendor SOC report, refer to 2025 finding #15.

2024-017: Certain General IT Controls for PHLContracts Still Require Strengthening

Prior Condition: The Procurement Department lacked a formal change management policy for PHLContracts.

Remediation Status: **Not Remediated** - During the current assessment, PHLContracts was unable to provide a formalized change management procedure or evidence of a defined process to communicate or enforce change management performance and documentation standards. As a result, this finding is considered partially remediated, refer to 2025 Finding #4.

Management Response:

CITY OF PHILADELPHIA

OFFICE OF THE DIRECTOR OF FINANCE
Room 1330 Municipal Services Building
1401 John F. Kennedy Boulevard
Philadelphia, PA 19102
(215) 686-6140
FAX (215) 568-1947

ROB DUBOW
Director of Finance

ACIS

Inadequate Change Management Documentation and Segregation of Duties

Recommendations: Management should ensure that all change management requests are fully documented, including evidence of testing, management approval, and identification of the individual who migrated the change to production. In addition, management should implement controls to enforce segregation of duties between development and production migration activities, including preventing users from promoting their own changes into production.

Management View: The Office of Innovation and Technology (OIT) is already using TeamDynamix as the ITSM for Change Management. Moving forward, ACIS will also adopt TeamDynamix as part of its Change Management procedures to maintain a complete audit trail of change requests, approvals, implementation details, and supporting evidence. This ensures consistency with enterprise change control standards and provides traceability for all future changes.

In addition, OIT published Change Management artifacts documentation standards to improve audit readiness and operational transparency. This includes the development of standardized artifacts and more consistent retention of review evidence, approvals, and remediation records.

Contact Information: Nicole Cook, Compliance Officer, Office of Innovation and Technology, (267) 432-1643

Inadequate Documentation and Evidence Supporting User Access Termination and Access Reviews

Recommendation: Management should formalize and document procedures for user access termination to ensure timely removal of access and retention of supporting documentation. Additionally, management should document the methodology used to compile and validate the completeness of the user population used as part of the user access review, retain evidence of reviewer approval, and document all access changes resulting from the review.

Management View: The Office of Innovation and Technology (OIT) will monitor all new production implementations, user activations, and user terminations for ACIS to ensure that each action is supported by a documented change request or ticket with the appropriate approvals. TeamDynamix (TDX) is already used as the enterprise system for submitting and approving user activation and termination requests, and this monitoring will verify that a complete and accurate ticket trail exists for all account lifecycle events. Tracking and oversight of these activities will begin immediately, and the relevant IT management team will review compliance on an ongoing basis and address any exceptions identified.

In addition, OIT is currently formalizing a User Access Review (UAR) on a quarterly basis for ACIS, ADPICS, and FAMIS. A list of all active users in these systems will be generated and sent to the respective system administrators, who will distribute the lists to each department liaison for validation. These administrators will distribute the lists to each department liaison for validation.

Departments will identify users who should no longer have access, and tickets will be created to disable those accounts. After remediation, a new set of user lists will be generated to confirm that all required deactivations have been completed and that the UAR is current. Departments will provide email confirmation once their reviews are complete. OIT management is expecting to have this completed by FY2027 Q2.

OIT also published User Access Management and UAR artifacts documentation standards to improve audit readiness and operational transparency. This includes the development of standardized artifacts, clearer guidance for reviewers, and more consistent retention of review evidence, approvals, and remediation records.

Contact Information: Nicole Cook, Compliance Officer, Office of Innovation and Technology, (267) 432-1643

PHLContracts

Inadequate Documentation and Execution of Privileged Access Provisioning, Termination, and User Access Reviews

Recommendation: Management should formalize and document procedures for privileged access provisioning, including retention of approval and business justification. In addition, management should strengthen termination controls to ensure timely access removal and retention of supporting documentation. Finally, management should implement a periodic UAR process that includes review of all access, evaluation of roles and associated permissions, and identification of incompatible role assignments to determine that the access is still considered appropriate. The review should be formally documented, include evidence of the completeness and accuracy of procedures performed, reviewer approval, and capture any access changes or remediation actions resulting from the review.

Management View: The Procurement Department agrees that documentation of access controls within PHLContracts has been deficient and that user access reviews have been inconsistent. The department is addressing this twofold: 1) by collecting additional supporting documentation for privileged access provisioning and 2) establishing formalized, periodic user access reviews (UARs) to improve access governance.

Procurement maintains an electronic form to document all user access requests and updates for PHLContracts, and the Department will make improvements to document approval and business justification for privileged access. All documentation will be stored electronically, made available, and retained to support audit requirements. The Department will also work to improve termination controls to revoke access in a timely manner and ensure documentation of access removal is maintained prior to being identified during periodic UARs.

Contact Information: Kameron Stopfer, Deputy Commissioner, Procurement Department, (215) 686-4744

VENDOR-PUSHED CHANGES ARE NOT FORMALLY APPROVED OR ACKNOWLEDGED

Recommendations: Management should establish procedures to obtain a complete population of changes from the system when required, formally approve or acknowledge vendor-pushed changes, and perform post-implementation verification to confirm changes were implemented successfully. Supporting documentation should be retained to demonstrate management oversight of change management activities.

Management View: The Department concurs that vendor-pushed changes to PHLContracts should be consistently documented and acknowledged. Procurement does currently review all system changes implemented by the vendor (though there was an acknowledgement response that was missed during the audit period). In response, Procurement will define the process to improve change management controls, including working with the vendor to review, acknowledge, and document all system enhancements and maintain a complete record of such

changes prior to implementation. Post-implementation, all changes will be validated to ensure they are implemented as intended and address any consequent issues.

Contact Information: Kameron Stopfer, Deputy Commissioner, Procurement Department, (215) 686-4744

INADEQUATE REVIEW OF SOC 1 REPORT

Recommendations: Management should establish and document procedures for reviewing SOC reports, including evaluation of the auditor's opinion and exceptions (if any), identification of relevant complementary user entity controls and if applicable obtain associated bridge letters. Evidence of the review should be retained to demonstrate management oversight and support reliance on third-party service providers.

Management View: Procurement agrees with the need for a documented, comprehensive review of SOC reports. The Department is establishing a defined process for the timely acknowledgement and review of the SOC 1 reports, which will include an evaluation of the auditor's opinion and findings, along with any noted exceptions or deficiencies.

Contact Information: Kameron Stopfer, Deputy Commissioner, Procurement Department, (215) 686-4744

OFFICE OF INNOVATION AND TECHNOLOGY (OIT)

LACK OF PERIODIC USER ACCESS REVIEWS

Recommendations: Management should implement a periodic UAR process that includes review of standard and privileged users, evaluation of roles and associated permissions, and identification of incompatible role assignments to determine that the access is still considered appropriate. The review should be formally documented, include evidence of the completeness and accuracy of procedures performed, reviewer approval, and capture any access changes or remediation actions resulting from the review.

Management View: The Office of Innovation and Technology (OIT) is formalizing an automated User Access Review ("UAR") campaign for Active Directory and Entra ID focused on privileged access every 90 days as part of ongoing efforts to strengthen access governance. Although privileged access reviews have been performed since the beginning of FY2026, this initiative introduces a more structured, consistent, and automated process to improve efficiency and accuracy. Automated workflows will be leveraged to support accuracy and timely completion, and system owners and managers will retain responsibility for performing a thorough review of all elevated permissions to confirm that privileged access remains aligned with a valid and current business need.

In addition, OIT is initiating a formal UAR campaign over standard user access. By formalizing the process, this will reinforce the principle of least privilege, enhance oversight of user entitlements, and ensure that access rights remain aligned with job responsibilities and operational requirements.

OIT also published UAR artifacts documentation standards to improve audit readiness and operational transparency. This includes the development of standardized artifacts, clearer guidance for reviewers, and more consistent retention of review evidence, approvals, and remediation records.

Contact Information: Nicole Cook, Compliance Officer, Office of Innovation and Technology, (267) 432-1643

FAMIS & ADPICS

LACK OF SEGREGATION OF DUTIES BETWEEN TEST AND PRODUCTION ENVIRONMENTS

Recommendations: Management should implement controls to enforce segregation of duties between test and production environments, including restricting users from promoting their own changes. In addition, management should establish monitoring and documentation requirements to ensure production migrations are reviewed, approved, and performed by authorized individuals.

Management View: The Office of Innovation and Technology (OIT) noted that ACIS will also adopt TeamDynamix (TDX) as part of its formal Change Management procedures to address the segregation-of-duties gap identified between the test and production environments. All changes, including those moving from test to production, will require a documented TDX change request with appropriate approvals, implementation details, and supporting evidence to ensure a complete audit trail.

Segregation of duties will also be enforced within TDX so that individuals responsible for testing changes cannot be the same individuals approving or promoting those changes into production.

OIT also published Change Management artifacts documentation standards to improve audit readiness and operational transparency. This includes the development of standardized artifacts and more consistent retention of review evidence, approvals, and remediation records.

Contact Information: Nicole Cook, Compliance Officer, Office of Innovation and Technology, (267) 432-1643

UNTIMELY REMOVAL OF USER ACCESS AND MISSING TERMINATION DOCUMENTATION

Recommendations: Management should redesign termination controls and communicate to the associated stakeholders the updated process to ensure user access is removed promptly upon termination and that documentation evidencing approval and completion of access removal is retained in accordance with access management policies.

Management View: The Office of Innovation and Technology (OIT) will monitor all new production implementations, user activations, and user terminations for ADPICS and FAMIS to ensure that each action is supported by a documented change request or ticket with the appropriate approvals. TeamDynamix (TDX) is already used as the enterprise system for submitting and approving user activation and termination requests, and this monitoring will verify that a complete and accurate ticket trail exists for all account lifecycle events. Tracking and oversight of these activities will begin immediately, and the relevant IT management team will review compliance on an ongoing basis and address any exceptions identified.

OIT also published User Access Management and UAR artifacts documentation standards to improve audit readiness and operational transparency. This includes the development of standardized artifacts, clearer guidance for reviewers, and more consistent retention of review evidence, approvals, and remediation records.

Contact Information: Nicole Cook, Compliance Officer, Office of Innovation and Technology, (267) 432-1643

LACK OF PERIODIC USER ACCESS REVIEWS (ADPICS)

Recommendation: Management should implement a periodic UAR process for ADPICS that includes review of standard and privileged users, evaluation of roles and associated permissions, and identification of incompatible role assignments to determine that the access is still considered appropriate. The review should be formally documented, include evidence of the completeness and accuracy of procedures performed, reviewer approval, and capture any access changes or remediation actions resulting from the review.

Management View: The Office of Innovation and Technology (OIT) is currently formalizing a User Access Review (UAR) on a quarterly basis for ACIS, ADPICS, and FAMIS. A list of all active users will be generated and sent to system administrators, who will distribute the lists to each department liaison for validation. Departments will identify users who should no longer have

access, and tickets will be created to disable those accounts. After remediation, a new set of user lists will be generated to confirm that all required deactivations have been completed and that the UAR is current. Departments will provide email confirmation once their reviews are complete. OIT management is expecting to have this completed by FY2027 Q2.

OIT also published User Access Management and UAR artifacts documentation standards to improve audit readiness and operational transparency. This includes the development of standardized artifacts, clearer guidance for reviewers, and more consistent retention of review evidence, approvals, and remediation records.

Contact Information: Nicole Cook, Compliance Officer, Office of Innovation and Technology, (267) 432-1643

INADEQUATE DOCUMENTATION SUPPORTING USER ACCESS REVIEWS (FAMIS)

Recommendation: Management should formalize documentation requirements for UARs, including a review of all users, evaluation of roles and associated permissions, and identification of incompatible role assignments to determine that the access is still considered appropriate. The review should be formally documented, include evidence of the completeness and accuracy of procedures performed, reviewer approval, and capture any access changes or remediation actions resulting from the review.

Management View: The Office of Innovation and Technology (OIT) is currently formalizing a User Access Review (UAR) on a quarterly basis for ACIS, ADPICS, and FAMIS. A list of all active users in FAMIS, ADPICS, and ACIS will be generated and sent to the respective system administrators. These administrators will distribute the lists to each department liaison for validation. Departments will identify users who should no longer have access, and tickets will be created to disable those accounts. After remediation, a new set of user lists will be generated to confirm that all required deactivations have been completed and that the User Access Review (UAR) is current. Departments will provide email confirmation once their reviews are complete. OIT management is expecting to have this completed by FY2027 Q2.

OIT also published User Access Management and UAR artifacts documentation standards to improve audit readiness and operational transparency. This includes the development of standardized artifacts, clearer guidance for reviewers, and more consistent retention of review evidence, approvals, and remediation records.

Contact Information: Nicole Cook, Compliance Officer, Office of Innovation and Technology, (267) 432-1643

Basis2

Recommendations: Management should ensure that all production migrations are supported by complete documentation, including evidence of pre-implementation testing and management approval. Documentation should be retained in accordance with change management policies to demonstrate effective oversight.

Management View: The Office of Innovation and Technology (OIT) acknowledges that Basis2 Leadership concurs with this finding. Change management controls have been in place since April 2026, when this finding was identified. The teams that test development work are no longer allowed to move items to production in the same development release. All production migrations now require explicit approval documented within the ticket from designated leadership roles (Product Owner, Technical Manager, IT Director, or Deputy Commissioner/designee), and releases will not proceed without this approval. The Release Management process created previously was amended in response to this finding, and the complete process is now being followed, as Basis2 Leadership monitors this process during the weekly production support meetings.

Contact Information: Nicole Cook, Compliance Officer, Office of Innovation and Technology, (267) 432-1643

UNREVOKED ACCESS FOR TERMINATED EMPLOYEES AND CONSULTANTS

Recommendation: Management should strengthen termination controls by implementing procedures to address potential spelling differences to ensure timely notification of terminations, and prompt removal of system access. Where feasible, termination processes should be automated or integrated with HR systems to reduce reliance on manual processes.

Management View: The Office of Innovation and Technology (OIT) acknowledges that Basis2 Leadership identified the deficiency related to delayed termination of user access within the Basis2 system. The root causes identified include reliance on manual processes, dependency on name-based matching (which is susceptible to spelling variations), and inconsistent communication of termination events.

To address these issues, management plans to take the following steps:

- Complete a root cause analysis of the legacy termination files to find out if a more accurate tracking method is possible. The aim is to shift from relying on names to using a unique identifier, such as employee ID, whenever possible. This will also include checks for spelling differences.
- Improve how terminations are communicated by setting up a formal process for notifying the Basis2 support team promptly. The process will clarify who is responsible and outline what to do if issues come up.
- Put in place regular monitoring controls, such as monthly reconciliations between HR termination records and active Basis2 users, to spot and fix any mismatches.
- As part of next year's planning cycle (FY27), look into ways to automate and potentially integrate the HR system with Basis2, aiming to cut down on manual work.

Timeline:

- Immediate process updates and communication protocols: Q3 FY26
- Reconciliation control implementation: Q3 FY26
- Automation/integration assessment: FY27 planning cycle
- Management will track progress through internal control monitoring and report status as part of ongoing audit remediation efforts.

Contact Information: Nicole Cook, Compliance Officer, Office of Innovation and Technology, (267) 432-1643

LACK OF PERIODIC USER ACCESS REVIEWS

Recommendation: Management should implement a periodic UAR process for Basis2 that includes review of standard and privileged users, evaluation of roles and associated permissions, and identification of incompatible role assignments to determine that the access is still considered appropriate. The review should be formally documented, include evidence of the completeness and accuracy of procedures performed, reviewer approval, and capture any access changes or remediation actions resulting from the review.

Management View: The Office of Innovation and Technology (OIT) acknowledges that Basis2 Leadership concurs with the findings current user access review process did not consistently retain documentation or validate access appropriateness. In response, a formal review process is being implemented.

Beginning April 2026, reviews will include:

- Monthly review of privileged users and periodic review of standard users
- Retention of user listings, approvals, and access changes

Role-to-permission mappings will also be reviewed to ensure appropriate access and identify conflicts. These reviews will be documented.

Contact Information: Nicole Cook, Compliance Officer, Office of Innovation and Technology, (267) 432-1643

ONEPHILLY

INADEQUATE USER ACCESS REVIEW PROCESS

Recommendations: Management should formalize and implement a UAR process for OnePhilly that mandates reviewer responses, documents the completeness and accuracy of the user population, and ensures timely completion and documentation of access modifications resulting from the review. Additionally, management should review and approve the segregation of duties policy and roles matrix annually, every fiscal year.

Management View: The Office of the Director of Finance, in coordination with OnePhilly, acknowledges the need to further formalize and strengthen the user access review (UAR) process. OnePhilly currently utilizes a centralized dashboard to facilitate departmental review of user access, track responses, and monitor remediation activities.

To enhance the control environment, OnePhilly is implementing a formalized UAR process that will require documented reviewer responses, validation of the completeness and accuracy of the user population, and retention of evidence supporting reviewer approval and access modifications. The process will also ensure the timely completion of reviews and the documentation of any remediation actions resulting from the review.

In addition, management will formalize the annual review and approval of the segregation-of-duties policy and roles matrix to ensure continued alignment with system access and control requirements. Documentation of these reviews will be retained to support audit and compliance expectations.

Contact Information: Shipra Jha, Director of OnePhilly, Office of The Director of Finance, (215) 380-4248

INADEQUATE REVIEW OF SOC 1 REPORT

Recommendation: Management should establish and document procedures for reviewing SOC reports, including evaluation of the auditor's opinion and exceptions (if any), identification of relevant complementary user entity controls and if applicable obtain associated bridge letters. Evidence of the review should be retained to demonstrate management oversight and support reliance on third-party service providers.

Management View: The Office of the Director of Finance, in coordination with OnePhilly, acknowledges the need to formalize and document the review of SOC 1 reports. OnePhilly is implementing a structured review process to be performed on a bi-annual basis in coordination with its managed services provider.

This process will include evaluation of the auditor's opinion, review of any noted exceptions, identification of relevant complementary user entity controls, and, where applicable, obtaining bridge letters to ensure coverage over the audit period. Documentation of the review will be retained to evidence management oversight and support reliance on third-party service providers.

Contact Information: Shipra Jha, Director of OnePhilly, Office of The Director of Finance, (215) 380-4248

PRISM

INADEQUATE DOCUMENTATION AND SEGREGATION OF DUTIES FOR PRODUCTION MIGRATIONS

Recommendations: Management should enforce segregation of duties controls to ensure individuals developing or testing changes cannot migrate those changes to production. In addition, management should implement monitoring controls and retain documentation, evidencing independent review of production migrations.

Management View: Change management controls have been established in response to this finding to address gaps in approval, documentation, and segregation of duties. Segregation of duties has been enforced such that individuals responsible for development and testing are prohibited from executing production migrations for the same release. All production migrations now require documented, explicit approval within the ticket from designated PRISM leadership roles (Product Owner, Technical Manager, IT Director, or Commissioner/designee), and releases will not proceed without this approval. The previous Release Management process was updated to incorporate these requirements, and the revised procedures have been in place since March 25, 2026. Compliance with these controls is formally monitored and documented by PRISM Leadership through weekly production support meetings, which include reviews of approval evidence and adherence to segregation of duties requirements.

Contact Information: Kathleen McColgan, Revenue Commissioner, Revenue Department, (215) 686-6400

Lack of Executive Approval for Emergency Application Changes

Recommendations: Management should ensure that all emergency application changes are supported by documented executive approval in accordance with the change management policy. Change tickets should be updated to require and retain evidence of such approvals prior to implementation.

Management View: The off-schedule release (emergency changes moved to production) process was updated in response to this finding, and the complete process is now being followed as of March 25, 2026. Each time an emergency change is requested, it is documented and will not be released without formal approval from the PRISM Leadership team. Emergency changes require documented approval within the ticket from designated PRISM leadership roles (Product Owner, Technical Manager, IT Director, or Commissioner/designee), are deployed by a separate release function to maintain segregation of duties, and are subject to documented post-release review during weekly production support meetings to ensure proper oversight and monitoring of emergency activity.

If the PRISM Leadership team is unavailable for the emergency change, the Revenue Commissioner may approve an exception allowing the Technical Architect to expedite the change; such approval must be documented within the ticket and is subject to the same post-implementation review and oversight controls.

Contact Information: Kathleen McColgan, Revenue Commissioner, Revenue Department, (215) 686-6400

INADEQUATE USER ACCESS REVIEW PROCESS

Recommendations: Management should formalize and implement a periodic UAR process for PRISM that includes documented validation of population completeness, review of standard and privileged users, evaluation of roles and associated permissions, and identification of incompatible role assignments. The review should be formally documented, include evidence of reviewer approval, and capture any access changes or remediation actions resulting from the review.

Management View: PRISM Leadership concurs that the current user access review process did not consistently retain documentation or validate the appropriateness of access. In response, a formal review process is being implemented.

Beginning April 2026, reviews will include:

- Monthly review of privileged users and annual review of standard users, with results formally documented, reviewed, and remediated; formal written procedures will be finalized and maintained
- Retention of user listings, approvals, and access changes

Role-to-permission mappings will also be reviewed to ensure appropriate access and to identify potential conflicts or incompatible access combinations. These reviews will be formally documented, approved, tracked, and remediated as part of the ongoing access governance process.

Contact Information: Kathleen McColgan, Revenue Commissioner, Revenue Department, (215) 686-6400

INADEQUATE REVIEW OF SOC 1 REPORT

Recommendations: Management should establish and document procedures for reviewing SOC reports, including evaluation of the auditor's opinion and exceptions (if any), identification of relevant complementary user entity controls and if applicable obtain associated bridge letters. Evidence of the review should be retained to demonstrate management oversight and support reliance on third-party service providers.

Management View: PRISM Leadership concurs with the findings and has implemented a formal, documented process for reviewing, retaining, and documenting the SOC report moving forward. This process has been in place as of March 2026, including evaluation of the auditor's opinion, relevant control considerations, and identification of complementary user-entity controls, with documentation retained to evidence the review.

Contact Information: Kathleen McColgan, Revenue Commissioner, Revenue Department, (215) 686-6400