



City of Phoenix

Mission Statement

To improve the quality of life in Phoenix through efficient delivery of outstanding public services.

Project Team

Aaron Cook
City Auditor

Stacey Linch
Deputy City Auditor

Mahdi Lasker
Sr. Internal Auditor – IT

Judith Onayemi
Sr. Internal Auditor - IT

Project Number

1250007

This report can be made available in alternate format upon request.

**Retirement Office
Application Controls - PensionGold**

October 11, 2024

Report Highlights

Application Controls

Appropriate input, output, and processing controls were in place to ensure application data integrity.

General Controls

Appropriate access controls, audit logging, encryption, and data backup controls were in place to ensure application integrity and security.

*City Auditor Department
140 N 3rd Avenue Phoenix, AZ 85003
602-262-6641 (TTY use 7-1-1)*

Executive Summary

Purpose

Our purpose was to validate key system controls in the new PensionGold application to ensure confidentiality, data integrity, and availability.

Background

PensionGold is the City's retirement administration system, used by the Retirement Office (Retirement). City employees belong to the City of Phoenix Employees' Retirement System (COPERS). PensionGold manages all aspects of retirement for COPERS Members.

In 2020, the City entered into an agreement with Levi, Ray & Shoup, Inc. (LRS) to upgrade its existing PensionGold system for \$6.2M. The application will eventually provide a website for members to log in and view their individual retiree account information. As of March 2024, LRS has delivered the PensionGold Version 3. primarily used by Retirement staff for various account maintenance activities, including benefit payment calculations, account maintenance, service purchase requests, and member correspondence.

Our audit focused on the following areas:

- **Application Controls (input/output/processing)** – fields within the application and system interfaces were working as designed.
- **Access Controls** – access was authorized and granted with the least privilege needed to perform their job.
- **Password Management** – password controls restricted unauthorized access.
- **Other General Controls** – application logging and encryption were enabled.

Results in Brief

Key application controls were working as designed. No deficiencies were noted.

We inspected a sample of input, output, and processing controls for PensionGold and found:

- Input controls were in place to ensure data accuracy.
- Processing controls were in place to ensure new members were automatically imported into the system with accurate member information.
- Output controls were in place to ensure correspondence letters displayed the correct member information.

System access was appropriately authorized and consistent with employees' job duties.

User account management practices were appropriate to ensure access was only provided to individuals with a valid business need and that access rights were appropriate. We also validated that administrative rights were only provided to those individuals with a valid business need. Controls were in place for user account management.

Strong access controls, including multifactor authentication, were in place for PensionGold.

Password requirements were strong and matched the City's password standards. The application also includes multifactor authentication controls to comply with City Information Technology (IT) standards.

Application logging and information security controls for PensionGold complied with City standards.

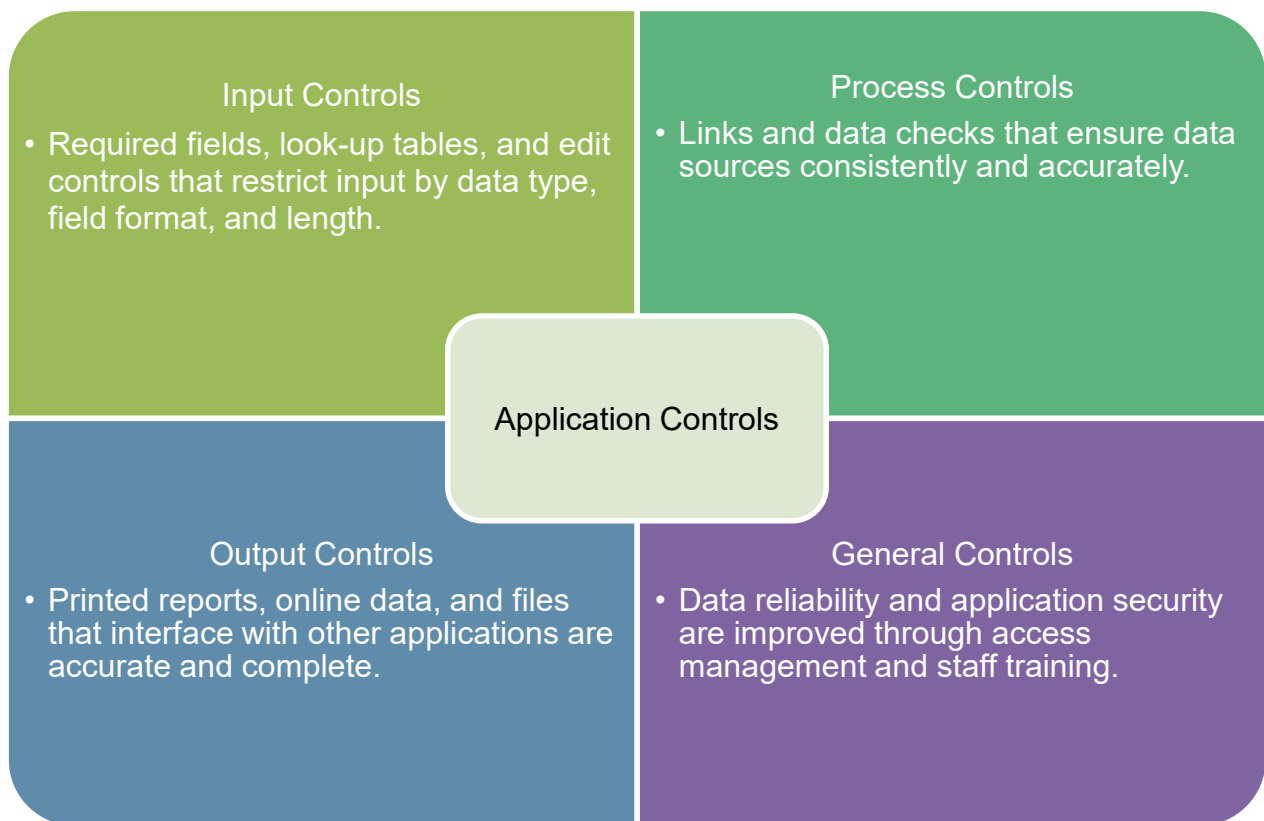
We verified that application logging was enabled to log the transaction date, time, and name of the user who performed the transaction and confirmed that users could not edit the logs. Additionally, appropriate controls were in place for data encryption and backup and recovery.

1 – Application Controls

Background

Administrative Regulation (A.R.) 1.84 – Information Security Management requires departments to implement controls to protect their information systems. Application controls are security measures implemented within a software application to ensure the integrity, accuracy, completeness, and confidentiality of data. The controls listed below help prevent unauthorized access, data errors, fraud, and other security risks:

Examples of System Controls



Application controls can help ensure data reliability and system security.

We reviewed the application controls for PensionGold by testing fields that accept identifying information. Additionally, to better understand the application control risks, we reviewed application design documents, interviewed staff, and performed testing on a sample of controls.

Results

Key application controls worked as designed. We did not identify any deficiencies.

To validate key system controls we:

- Reviewed system-generated member correspondence to check whether the information on the document matched the employee profile.
- Inspected a sample of department reports to check whether data output matched the source data (i.e., eCHRIS).
- Verified whether a sample of new hires were automatically given a profile in PensionGold.

We tested a sample of input, output, and processing controls to determine if the controls were working. The details of our testing are as follows.

Input Controls

Input controls prevent users from entering inaccurate information into the system. For example, an application field designed to accept social security numbers (SSN) would be expected to prevent alphabetic characters, while a date of birth field should contain only digits that correspond to a date on the calendar. Input controls ensure application integrity and reduce the risk of user error. We inspected the name, SSN, employee identification number, and date of birth fields and verified that all fields had appropriate character rules and limitations. We attempted to run queries in the application using numeric characters in fields designed to accept alphabetic entries and vice versa, and noted that the application did not permit the entry.

In addition, we validated the following:

- The date range for image searches was limited to 90 days and was working as designed.
- Users could not manipulate drop-down fields.
- Member information lookup field lengths were appropriate.
- Address changes were validated using a third-party feature integration.

Processing Controls

Processing controls ensure that actions within the application and interfaces between other applications are executed accurately. Without processing controls, transactions may not be processed accurately, leading to incorrect data. One of the key processing functions for PensionGold is the interface with the City's payroll system, eCHRIS. Employee data from eCHRIS is sent to PensionGold each pay period. This data is used to track employment dates and salary information. To determine that the interface processing was functioning correctly, we compared a sample of 27 out of 416 employees hired between January 2024 - May 2024. All 27 members were found with a profile in PensionGold. The member information such as employee name, identification

number, last four digits of their SSN, department name, and labor unit in eCHRIS matched PensionGold for all 27 members.

Another good processing control in PensionGold is the creation of a barcode when staff correspond with members. When the correspondence is returned by the member, staff can scan the barcode to locate the member's account to map the document back to the member's profile. This control helps ensure that profile updates are applied to the correct member account. Due to technical difficulties, the barcode system could not be tested, but we plan to assess this control in a future audit.

Output Controls

Output controls ensure that system-generated documents display accurate information. Data output from PensionGold includes various correspondence to members related to their pension benefits. Without adequate controls, members could be provided misinformation about their retirement benefits. We reviewed a sample of the five most frequent correspondence documents sent to members to verify if the information on the document matched PensionGold and found no exceptions.

- **Application for Retirement** – Used by members to officially apply for benefits.
- **Designation of Beneficiaries** – Used by members to designate primary and alternate beneficiaries.
- **Change of Address** – Used by members to update their physical and/or mailing address.
- **Beneficiary Contact Letter** – Used to notify members that they do not have a beneficiary on file.
- **Income Verification Letter** – Provides members with proof of benefits, which can be provided to a 3rd party requestor (i.e., mortgage lender).

Recommendations

None

2 – General Controls

Background

Administrative Regulation (A.R.) 1.84 – Information Security provides a framework to protect the confidentiality, integrity, availability, and accountability of information collected, stored, maintained, transmitted, and processed by the City. General controls ensure the protection of information from unauthorized access, corruption, and data theft. Additional City IT Standards that govern these controls include:

- *City IT Standard s1.11 – Security Incident Event Monitoring*
- *Enterprise IT Standard INF-103 – Change Management*
- *Enterprise IT Policy 200-006 – Encryption*

For PensionGold, we reviewed general controls, including application logging, encryption of data, change management, and backup and recovery controls. We interviewed staff, observed operations, and reviewed system documentation and independent audit reports to determine if general controls were in place to ensure the confidentiality, integrity, and availability of the application and data.

Results in Brief

Application logging and security controls for PensionGold complied with City IT Standard s1.11 – Security Incident Event Monitoring.

As a security measure, logging activities within an application should identify the transaction performed, the name of the user who performed the transaction, and the transaction date and time. Additionally, measures should be in place to prevent logs from being edited to ensure data integrity, and the application network time protocol (NTP) settings should ensure accurate time synchronization. Additional security controls include data encryption which prevents access to sensitive and personally identifiable information from unauthorized persons. Data backup and recovery services protect City data from loss and restores it when incidents occur.

Application Logging

Logging of activities is the process of tracking events or actions that have occurred in an application and is crucial to the security environment as the logged information can be used to troubleshoot issues, monitor system performance, and identify security events within an application.

City IT standard s1.11 – Security Incident Event Monitoring requires that departments:

- Log necessary information to ensure the confidentiality, integrity, and availability of City information systems.
- Log access to confidential information is logged for audit purposes.

- Quickly identify security incidents.
- Protect system logs from unauthorized access or tampering.
- Synchronize the time on logging hosts and central logging servers with the City's central time server.

We examined the different categories of logs within PensionGold, selected a sample of nine transaction entries, and verified that the transactions were logged with the date, time, and username of who performed the transaction. We also determined that users were unable to edit the logs and that the correct events were being logged.

Network Time Protocol Setting

The Network Time Protocol (NTP) setting is a very important security control to ensure accurate time synchronization within the system application. The PensionGold application is hosted within the cloud environment; therefore, we reviewed the application settings, which showed NTP synchronization was enabled.

Data Encryption

Data encryption prevents access to sensitive and personally identifiable information from unauthorized persons. We reviewed the vendor's Service Organization Report – Type II (SOC2) from July 2023 and verified that data was encrypted at rest using web browser-based communication secure sockets Layers (SSL) with certificate-based 256-bit encryption. The SOC report was issued prior to our audit scope. Therefore, we requested documentation (i.e., a bridge letter) from LRS attesting to the controls within the environment. No exceptions were noted.

Database Backup and Recovery

Backup and recovery plans are security controls that provide continuity after an incident that adversely impacts the application's security environment, thereby limiting downtime and overall loss to the business. We reviewed the SOC2 report and confirmed backup and recovery procedures were in place, including performing incremental backups daily and full backups weekly.

Change Management

Change management controls ensure that prior to application changes, standard procedures are followed. Change management procedures include ensuring changes are authorized, tested, and communicated to stakeholders. Changes made without control procedures could result in downtime that would impact application performance.

Enterprise IT Standard INF-103 – Change Management requires that change documentation includes:

- Description of the change
- Testing of the change

- Backout procedures
- Management approval

As PensionGold is a cloud-based application hosted and supported by Flexential, we focused our testing on verifying if there were procedures in place by the vendor to communicate to Retirement any major changes to the system and to allow staff the opportunity to review changes and, if applicable, approve or deny changes. We interviewed staff, reviewed documentation, and identified that changes requested by staff were documented through a Problem Incident Report form, which documented the scope of the change and the approval by Retirement. Additionally, we found that changes initiated by LRS were communicated to Retirement via email and in advance of the change. No exceptions were noted.

Recommendations

None

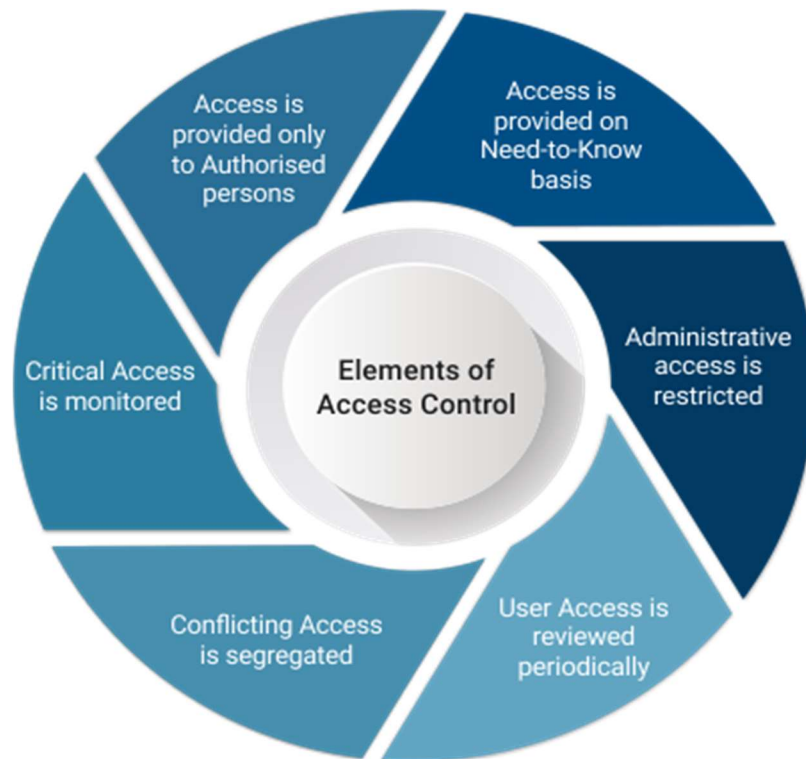
3 – Access Controls

Background

Access management controls determine who is authorized to access or perform actions in an application and is dependent on authentication, which confirms that the user is who they say they are. PensionGold is currently only accessible to Retirement staff. In the future, the MemberDirect module (a web-based portal for COPERS members to access their retirement information) will be put into production.

. Access management is governed by *City IT Standard s1.2 – Cloud Computing Standard* and *Enterprise IT Standards 200.201 – Identity Management, 300-015 – Password Management*.

Elements of Access Control



Access controls reduce the risk of unauthorized access to systems.

Results

Overall, strong access controls were in place for PensionGold. Enabling multifactor authentication will improve controls.

We interviewed staff, reviewed documentation, and performed testing to ensure controls were in place for user access provisioning, password management, and user access rights (i.e., least privilege enabled).




Access Provisioning

Access controls determine whether the user is allowed to carry out the action that they are attempting to perform, including any high-risk controls which may require proper segregation of duties. Staff provision, modify, and remove access using a problem incident report (PIR) form. We confirmed this process through the access granted to audit staff for testing. In addition to the test for access requests, we reviewed a sample of PIRs. We also reviewed the list of current employees who qualify for retirement, either voluntarily or involuntarily, by credited service. We determined that controls were in place for provisioning new users and segregation of duties.

Password Management

We compared the current password settings to *Enterprise IT Standard 300-015 – Password Management requirements*.

Password Compliance

City Requirement	Compliant
Password Length: at least 14 characters	
Password Complexity: <ul style="list-style-type: none"> • Uppercase alpha • Lowercase alpha • Numeric • Special character 	
Password Reuse: cannot be reused for 12 cycles	

City Requirement	Compliant
Password Interval: 90 days	✓
Account Lockout: after 5 failed login attempts	✓
Account Lockout Duration: locked out for at least 30 minutes	✓

Password configurations comply with City standards.

Multifactor Authentication (MFA)

City IT Standard s1.20 – Cloud Computing Standard requires appropriate multifactor authentication with cloud services. As a cloud-based application, this standard applies to PGV3. We noted that MFA was not initially enabled for users, but was implemented before the conclusion of our audit.

Recommendations

None

Scope, Methods, and Standards

Scope

We reviewed PensionGold Version 3 after its March 2024 go-live. We assessed application integrity, general data security, and identity management controls.

The internal control components and underlying principles that are significant to the audit objectives are:

- Control Activities
 - Management should design control activities to achieve objectives and respond to risks.
 - Management should design the entity's information system and related control activities to achieve objectives and respond to risk.
- Information & Communication
 - Management should internally communicate the necessary quality information to achieve the entity's objectives.
- Monitoring Activities
 - Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results.
- Control Environment
 - The oversight body should oversee the entity's internal control system.

Methods

We used the following methods to complete this audit:

- Reviewed scope of work vendor documents.
- Interviewed users of the application.
- Performed testing against a sample of controls.

Unless otherwise stated in the report, all sampling in this audit was conducted using a judgmental methodology to maximize efficiency based on auditor knowledge of the population being tested. As such, sample results cannot be extrapolated to the entire population and are limited to a discussion of only those items reviewed.

Data Reliability

The scope of this audit was to validate controls in PensionGold Version 3. We did this by (1) performing electronic testing, (2) reviewing existing information about the data and the system that produced them, and (3) interviewing agency officials knowledgeable about the data. We determined that this data was sufficiently reliable. In addition, we used employee information from the City's human resources system, eCHRIS. The eCHRIS data was previously determined to be reliable through an independent audit review.

Standards

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Any deficiencies in internal controls deemed to be insignificant to the audit objectives but that warranted the attention of those charged with governance were delivered in a separate memo. We are independent per the generally accepted government auditing requirements for internal auditors.