



City of Phoenix

Mission Statement

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

Project Team

Ross Tate
City Auditor

Aaron Cook
Deputy City Auditor

Jaki Gerald
Sr. Internal Auditor - IT

Project Number

1230033

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

Fire Department Application Controls – Ambulance Billing

August 1, 2023

Report Highlights

Application Controls

Strong automated and manual controls were present to help ensure data confidentiality, integrity, and accuracy.

General Controls

Staff adequately implemented change and service management controls. User account management is documented and monitored. Physical and environmental controls are in place.

***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 determine that application controls for the Phoenix Fire Department (Fire), Emergency Transportation Section (ETS), Respond Billing Application were in place and functioning to ensure data confidentiality, integrity, and availability.

Background

Fire provides ambulance transportation services for the City of Phoenix (City). Since 2006, ETS has provided billing and collection services for ambulance transports. In 2010, Fire entered into an agreement to use a billing application from TriTech called Sweet Billing. In 2018, TriTech merged with three other public sector software companies to form CentralSquare Technologies, LLC (CentralSquare). The ETS billing application was renamed Respond Billing with the most recent five-year service agreement signed on April 6, 2023. In 2022, Fire provided ambulance transport for over 83,658 individuals.

Results in Brief

Strong automated and manual controls were present to help ensure data confidentiality, integrity, and accuracy.

Respond Billing input controls ensured that call information was input accurately. Manual reconciliations ensured that no calls were missed and all services were coded. Application updates ensured codes and reasons were current. Respond Billing processing controls ensured that ETS' billing followed proper workflow. Approvals and role-based access controls provided segregation of duties and least privilege access.

General IT controls supporting the system were generally strong, with some opportunities for improvement regarding identity and password management.

We evaluated identity management, service level management, change management, backup and recovery, and physical and environmental controls. Overall, controls were functioning properly. There are opportunities for improvement, primarily around identity and password management controls. Regular review of access rights and group security settings should take place. Password requirements should be enhanced to meet the City's minimum standard.

Department Responses to Recommendations

Rec. #2.1: In compliance with <i>City IT Standard s1.5 – Password Management</i> , update password requirements to meet the City standard. If the password requirements cannot be met, request a waiver in accordance with <i>City IT Standard b.1.3 IT Waiver Standard</i> .	
Response: Password rules will be changed on the application to comply with the recommendation in the final audit report.	<u>Target Date:</u> 8/31/2023
Explanation, Target Date > 90 Days: NA	
Rec. #2.2: In compliance with <i>City IT Standard s1.3 – Identity Management</i> , ensure that appropriate ETS supervisors regularly perform a documented review of roles and access privileges in Respond Billing.	
Response: PFD ETS will work with Tech Services to create an auto-generated report from the application, including users and their roles. ETS Supervisors will use this report to conduct and document quarterly reviews of roles and access privileges and request changes if necessary.	<u>Target Date:</u> 9/30/2023
Explanation, Target Date > 90 Days: NA	
Rec. #2.3: Conduct a review of user groups access rights and role-based access configurations to ensure that they provide adequate data security and that segregation of duties is aligned with business objectives and compliance requirements.	
Response: PFD Tech services and ETS supervisors will work together to review each user's access rights and roles. Based on the review findings, the appropriate role access updates will be made to meet security and segregation of duties.	<u>Target Date:</u> 10/31/2023
Explanation, Target Date > 90 Days: NA	
Rec. #3.1: Consider installing a locked rack or cage to provide an additional layer of physical security to prevent unauthorized access to or tampering of the Respond Billing application and database servers.	
Response: The ETS billing server is on a rack that cannot be secured on the rear side due to retrofit requirement constraints. PFD Tech Services is working with ITS to migrate the server into the ITS MetroCluster anticipated by the end of the year assuming availability. Once the ETS billing server is migrated to the ITS MetroCluster, it will be secured and locked.	<u>Target Date:</u> 1/31/2024

Explanation, Target Date > 90 Days: Fire is requesting more time because we are dependent on the ITS team for availability to support the migration of the ETS billing server to the ITS MetroCluster. This is the best, most secure, and most efficient option for securing the ETS Billing server.

Rec. #3.2: Create desktop procedures to help staff consistently use the Respond Billing system to perform business functions.

Response: PFD ETS will create and distribute standardized desktop procedures for staff to help ensure the consistent use of the Respond Billing application.

Target Date:
10/31/2023

Explanation, Target Date > 90 Days: NA

1 – Input, Processing, and Output Controls

Background

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, errors in accuracy and processing, fraud, and other security risks:

- Input controls verify the accuracy and completeness of data entered into an application, such as validation checks for data types and field lengths.
- Processing controls ensure that data is processed correctly within an application. Includes error detection and correction, workflow routines, and audit trails that record processing activities and the identity of the staff involved.
- Output controls refer to the mechanisms used to monitor, measure, and regulate the results of a system or process to ensure desired outcomes.

Application controls are important in ensuring the security and reliability of the ETS billing process and are often mandated by regulatory requirements and industry best practices.

Results

Respond Billing’s input controls are effective in ensuring data accuracy.

Through testing, we observed that Respond Billing’s input controls successfully prevented the submission of invalid data in critical fields while allowing for efficient entry of legitimate calls for transport and customer account information. In addition, daily supervisory reconciliations of call data uploaded from Fire’s electronic patient records solution (ePCR), ensured no calls resulting in ambulance transport were missed. We validated the key input controls listed below.

Key Input Controls

Input Control	Ensures accuracy by:	Respond Billing Examples:
Automated Interface	Runs a defined set of instructions to import data regularly.	Calls for transport are initially electronically imported into Respond Billing from ePCR.
Manual Reconciliation	Reconciles data imported to original source documentation.	ETS Prebilling section reconciles imported calls to ambulance history reports.
Validity Logic Checks	Checks data against another source or rule.	Address must be verifiable; SSN must not be null.

Input Control	Ensures accuracy by:	Respond Billing Examples:
		Call date must be between 2000 and 2030.
Field Checks	Accepts only the correct type of data (alpha, numeric, etc.).	"Amount" field must be numeric.
Closed Loop Verifications	Uses input data to pull up and display other relevant information.	Reason codes and credit IDs pull up descriptions when entered.
Dropdown List / Radio Button, Checkbox	Limits input to only a few options.	Batch owner is a dropdown list of staff with cash posting permissions.
Warnings / Hard Stops	Presents a warning box that can be bypassed or not depending on rules.	If an address cannot be verified a warning is displayed.
Automatic Calculation	Calculates and displays totals based on input.	"Total Charges", "Posted Cash" and "Remaining Cash" are automatically calculated.
Completeness Check	Requires all fields have been entered to move forward.	"Remaining Cash" field must be \$0.00 to post a batch.

Processing controls are effective in ensuring the accuracy and completeness of the ETS billing function.

Respond Billing has several layers of controls integrated into its processing workflow. In addition, these controls are supplemented by two daily error detection routines known as the "Ticket Scrubber" and the "Cash Batch Exception Report." Based on our testing, these error detection routines, combined with the controls listed below, work together to reduce the risk of inaccurate or incomplete ambulance transport billings.

Key Processing Controls

Processing Control	Ensures Accuracy by:	Respond Billing Examples:
Record Validation	Compares data input to external or internal sources for data duplication.	Respond Billing compares account information for each new patient and identifies potential duplicate accounts. Staff reviews and determines if the call belongs to a

Processing Control	Ensures Accuracy by:	Respond Billing Examples:
		pre-existing account or if a new account is needed.
Error Detection	Reconciles data entered to original source documentation.	Bolt-on Ticket Scrubber and Cash Batch Exception Reports identify common errors.
Audit Trails	Records processing activities, such as date and user id in an unmodifiable log.	Patient and call histories display every action taken. Entries in the histories cannot be modified or deleted.
Encryption	Secures data at rest and in transit so it can only be accessed by authorized staff.	The database server for Respond Billing is encrypted at rest and data is encrypted in transit.
Segregation of Duties	Divides key tasks and processes among users to prevent a single user from having too much control or access. Using RBAC (Role-based access controls) ensures that segregation of duties can't be bypassed.	RBAC in Respond Billing prevents access to certain tabs and fields and processes based on assigned profiles - including Billing, Cash Posting, Management, and System Administrators. However, a detailed configuration review has not been performed in recent years. A Chase Bank lockbox removes risk of acceptance of payments. Issuance of refunds and reconciliation to SAP is performed by Fire Fiscal staff.
Supervisor Reviews	Adds a layer of oversight to processing to identify errors or oversights.	Respond Billing's workflow requires many processes to be approved before moving to the next step.

Output controls are in place to ensure patient bills are accurate.

The final output in Respond Billing is a set of invoices that run each day and are mailed to the patients and / or insurance companies. We conducted sample testing of these invoices and found that they provided accurate patient and call information, and that charges and amounts due were calculated correctly.

Recommendations

None

2 – Identity and Password Management

Background

End users are an important part of an application's control environment because they ensure authorization and accountability. To mitigate the risks associated with end user activities, the City has established clear IT standards for user access in applications like Respond Billing. These include requirements for strong passwords as outlined in *City IT Standard s.1.5 – Password Standards* and requirements and restrictions on user identification and privileges documented in *City IT Standard s.1.3 – Identity Management*.

Results

Password requirements in Respond Billing do not meet the City's standard.

While Respond Billing includes several authentication requirements, it does not require complex passwords or prevent the reuse of passwords for at least 12 changes, as required by City Standard s.1.5 - Password Standards.

City IT Standard s.1.5 – Password Requirements

Requirement	Compliant
Minimum Length = 8 characters	Y
Minimum Interval = 60 days	Y
Password Complexity (upper/lower alpha, numeric, and special characters)	N
No Reuse = 12 changes	N
Failed Login = 5 attempts	Y

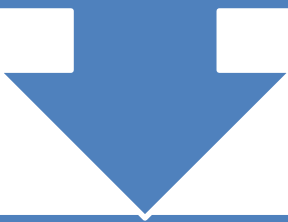
When an application cannot meet City IT standard requirements, a waiver should be completed in accordance with *City IT Standard b.1.3 – Waiver Standard*.

Identity management controls in Respond Billing are strong but could be improved by conducting reviews of user privileges more timely.

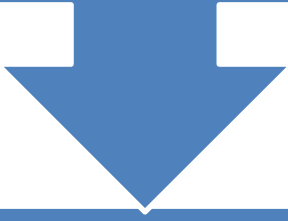
City Standard s.1.3 – Identity Management provides specific guidance for departments to following when managing user identities and access throughout the user account lifecycle, including account provisioning, routine monitoring, and decommissioning when access is no longer needed.

Identity Management Review Results

Account Provisioning		
Requirement		Testing Summary
Access requests should be approved and documented.	Yes	Requests for new access were documented in RemedyForce.
Least Privilege based access.	Yes	Role Based Access Control used.
Privileged accounts not used for everyday tasks.	Yes	Privileged accounts for IT staff only (SuperAdmin Accounts).



Monitoring		
Accounts suspended after 90 days of non-use.	Yes	All users logged in within last 30 days.
Privileges reviewed every 90 days.	No	Reviews have taken place, but are nine months behind schedule.



Decommissioning		
Disabled when access is no longer needed (termination, transfer)	Yes	All users were active Fire (ETS, Fiscal, IT) employees.

Reviewing user group security configurations regularly for Role-Based Access Control (RBAC) is important to ensure that they are still providing adequate segregation of duties.

RBAC configurations have not been reviewed since the system was originally implemented in 2010. As the application and billing functions evolve, changes in job roles, responsibilities, and workflows may require adjustments to RBAC configurations. In discussions with staff, there have been occasions when, due to staffing shortages, group rights have been extended in violation of segregation of duties to meet specific business needs. Formal processes were not in place to validate that those rights were later removed. Without regular reviews, security gaps may emerge, leading to the potential for unauthorized access to sensitive data or systems. By reviewing RBAC configurations, ETS can identify and address potential security risks, ensuring that access control policies align with their business objectives and compliance requirements.

Recommendations

- 2.1 In compliance with *City IT Standard s1.5 – Password Management*, update password requirements to meet the City standard. If the password requirements cannot be met, request a waiver in accordance with *City IT Standard b.1.3 IT Waiver Standard*.
- 2.2 In compliance with *City IT Standard s1.3 – Identity Management*, ensure that appropriate ETS supervisors regularly perform a documented review of roles and access privileges in Respond Billing.
- 2.3 Conduct a review of user groups access rights and role-based access configurations to ensure that they provide adequate data security, and that segregation of duties are aligned with business objectives and compliance requirements.

3 – Other General IT Controls

Background

An application's control environment refers to the set of policies, procedures, and controls established to ensure proper functioning and security of an application. It encompasses the people, processes, and technology that are used to support and maintain the application. The goal of the control environment is to ensure that the application operates as intended, and that it is protected from unauthorized access, modification, or destruction. This is typically accomplished by implementing a range of technical and administrative controls, such as training system users, data center physical and environmental controls, data encryption, and backup and recovery procedures.

Fire has a contract with the system vendor, CentralSquare, to provide ongoing support and maintenance. The contract includes a service level agreement (SLA). A well-written SLA helps mitigate risks associated with service disruptions and unauthorized access to data. We assessed the ETS control environment and governance structure to determine if it was sufficient to ensure the reliability and security of Respond Billing.

Results

The Respond Billing support and maintenance requirements contract includes important provisions to help ensure a strong control environment.

A well written SLA typically includes provisions to support confidentiality, data protection, support, and incident response.

SLA Provisions Supporting the Control Environment

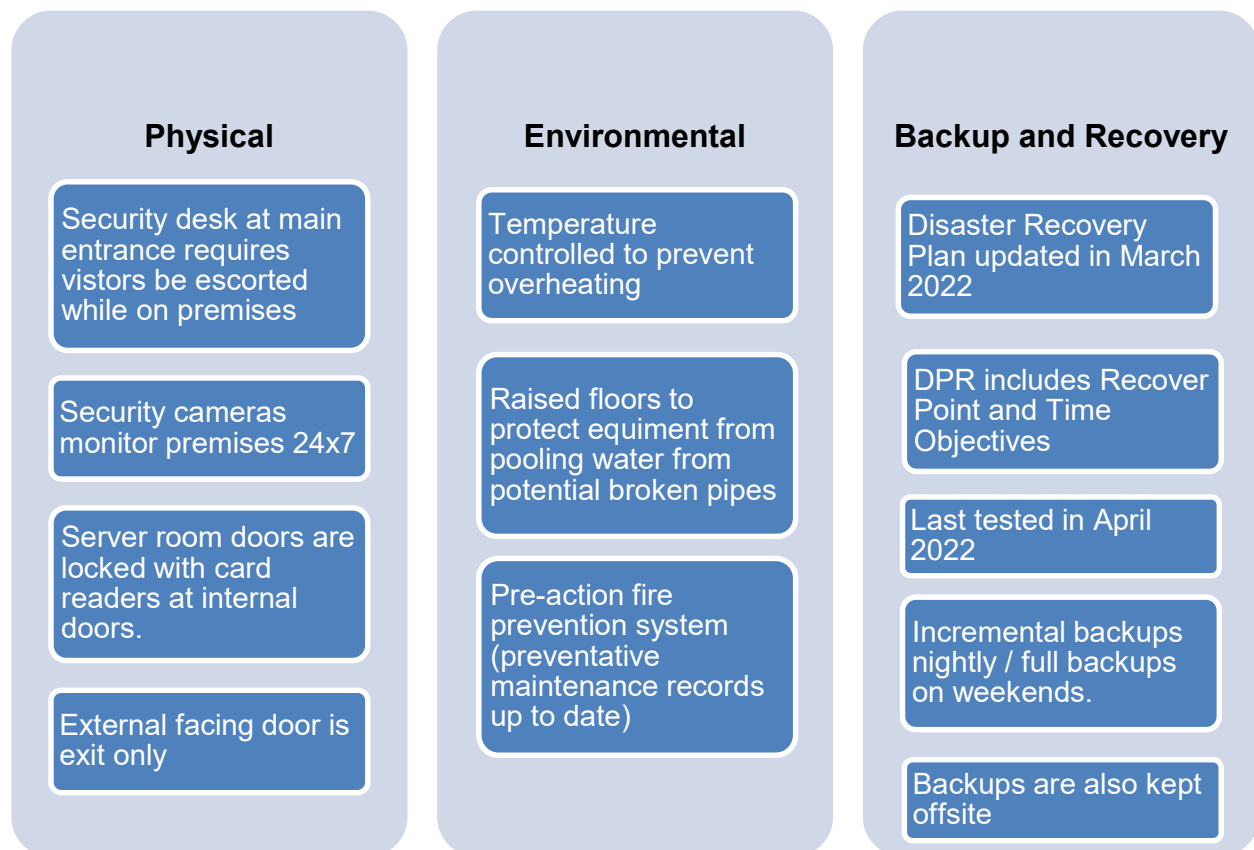
Confidentialty	Data Protection	Support	Incidents
<ul style="list-style-type: none">• Defined as all non-public, confidential, sensitive, or proprietary information• Can be disclosed orally, in writing, via electronic access• Disclosed only for uses approved in agreement	<ul style="list-style-type: none">• NIST SP800-53, ARS 18-552, ARS 44-7601, HITECH, PCI• Prohibits sub contracting• Requires 3rd party assessments SSAE 18, SOC2 or ISO/IEC 27001• Right to audit	<ul style="list-style-type: none">• Priorities and support response matrix• Priority levels• Issue definitions• Expected response times	<ul style="list-style-type: none">• Resolutions available• Priority levels• Defined Resolution Process• Resolution time requirements

The contract includes requirements regarding data protection and security, specifically around health records and criminal justice information. The contract also stipulates a prioritized response time to issues and incident resolution. We interviewed Fire IT staff, ETS management, and end users regarding vendor relations and did not identify any concerns. There have not been any reported data breaches or incidents.

Physical and environmental controls are in place and working to reduce the risk of environmental hazards such as fire, flood, and theft.

We verified that the following controls were in place through on-site observation, discussions with Fire IT support staff, and review of application dashboards, screen shots, and access control lists.

Physical and Environmental Controls in Place



Physical controls could be improved by making the rack storing the system be locked. Over 250 people have badge access to the data center where the server cluster holding the Respond Billing database is stored. Most are employees from Fire, the Public Works Department, ITS, or Police; but 37 active badges are assigned to contractors for janitorial, HVAC, or other necessary services. Due to the sensitive nature of the data

being stored, best practices for physical security, including locked racks within the data center, should be considered.

Service incidents and change requests are handled through the City's IT service management system, Remedyforce, as required by Citywide IT Standard b.1.11 – Change Management.

Use of Remedyforce ensures that important information regarding the incident or change is documented, and the required approvals are obtained. We reviewed all 124 incidents and five change requests related to the Respond Billing application for the July 2021 through March 2023. We found that:

- All change requests were prioritized, tested, had backout plans, and were properly approved.
- All incidents were prioritized and escalated as needed.

Our review indicated that, overall, Respond Billing application's availability and performance meets ETS' needs.

The Respond Billing databases are encrypted at rest and de-identified in transit between server and client.

The databases holding confidential patient and call information were encrypted at rest in 2021 and the primary index fields are also encrypted in transit to prevent patient and call identification.

Fire lacks current desktop operating procedures, increasing the risk that staff use the system inconsistently.

Desktop procedures help to ensure that end users conduct business properly and consistently when using Respond Billing. Staff could not provide any documented procedures, and believed any current documentation would be outdated. We found staff using personal notes to help them make sure to select the correct entries for some fields. Increased calls for ambulance services and staffing shortages since the pandemic have made it difficult for ETS to keep up with the increased workload and has led to a backlog of billing and collections. ETS' priority has been to address this backlog. As a result, policies and procedures have not been updated in recent years. Having current policies and procedures helps to ensure that billing is performed timely and efficiently, minimizing errors and customer disputes.

Recommendations

- 3.1 Consider installing a locked rack or cage to provide an additional layer of physical security to prevent unauthorized access to or tampering of the Respond Billing application and database servers.
- 3.2 Create desktop procedures to help staff consistently use the Respond Billing system to perform business functions.

Scope, Methods, and Standards

Scope

This audit covered application controls in place during fiscal year 2022-2023 for the Respond Billing application.

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

- Control Activities
 - Management should design the entity's information system and related control activities to achieve objectives and respond to risks.
- Risk Assessment
 - Management should identify, analyze, and respond to significant changes that could impact the internal control system.
- Control Environment
 - Management should demonstrate a commitment to recruit, develop, and retain competent individuals.
- Monitoring Activities
 - Management should remediate identified internal control deficiencies on a timely basis.

Methods

We used the following methods to complete this audit:

- Reviewed City IT standards and regulations, medical billing guides, organization charts, and prior internal audits.
- Reviewed system user guides, contracts, and vendor service agreements.
- Interviewed management and staff in the Fire Emergency Transportation and IT groups.
- Conducted an application and general controls risk assessment.
- Reviewed system generated reports and screenshots in the billing system and in the City's service management solution, Remedyforce.
- Tested report accuracy, administrative and technical review processes, and user account access control lists and access rights.
- Visited the Fire data center, inspecting physical and environmental 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

Data validation was an objective of this audit. We concluded that input, processing, and output controls, as well as general controls such as identity management and password management, provide sufficiently reliable data.

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.