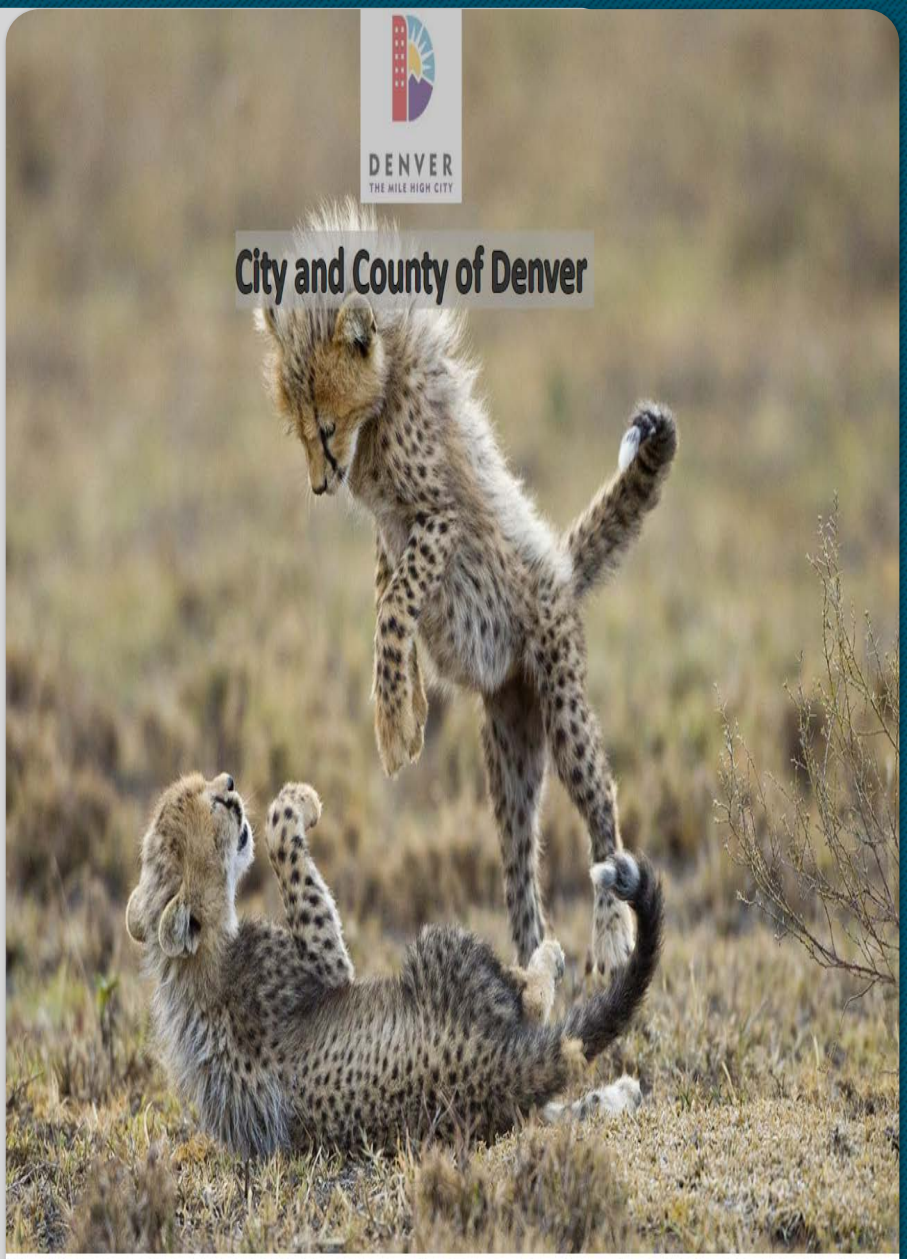
AUDIT REPORT
Technology Services and Department of Finance
GenTax System
April 2017



Office of the Auditor
Audit Services Division
City and County of Denver

Timothy M. O'Brien, CPA
Denver Auditor

FAST ENTERPRISES

The Auditor of the City and County of Denver is independently elected by the citizens of Denver. He is responsible for examining and evaluating the operations of City agencies and contractors for the purpose of ensuring the proper and efficient use of City resources, and providing other audit services and information to City Council, the Mayor, and the public to improve all aspects of Denver's government.

The Audit Committee is chaired by the Auditor and consists of seven members. The Audit Committee assists the Auditor in his oversight responsibilities regarding the integrity of the City's finances and operations, including the reliability of the City's financial statements. The Audit Committee is structured in a manner that ensures the independent oversight of City operations, thereby enhancing citizen confidence and avoiding any appearance of a conflict of interest.

Audit Committee

Timothy M. O'Brien, CPA, Chairman
Rudolfo Payan, Vice Chairman
Jack Blumenthal
Leslie Mitchell
Florine Nath
Charles Scheibe
Ed Scholz

Audit Management

Valerie Walling, CPA, CMC®, Deputy Auditor
Heidi O'Neil, CPA, CGMA, Director of Financial Audits
Dawn Wiseman, CRMA, Audit Manager

Audit Staff

Shannon Kuhn, CISA, IT Audit Supervisor
Nick Jimroglou, CISA, Lead IT Auditor
Jared Miller, CFE, Lead Auditor
Karin Doughty, CISA, Senior IT Auditor

You can obtain copies of this report by contacting us:

Office of the Auditor
201 West Colfax Avenue, #705
Denver CO, 80202
(720) 913-5000 ◆ Fax (720) 913-5247

Or download and view an electronic copy by visiting our website at: www.denvergov.org/auditor
Report number: **A2016-020**

City and County of Denver

201 West Colfax Avenue, #705 • Denver, Colorado 80202

720-913-5000 • Fax 720-913-5253 • www.denvergov.org/auditor

Timothy M. O'Brien, CPA
Auditor

April 20, 2017

AUDITOR'S REPORT

We have completed an audit of the City and County of Denver's tax collection system, GenTax. The objective of the audit was to determine the extent to which the GenTax application's administrative and systemic controls are designed to ensure data integrity and availability.

As described in the attached report, our audit indicated that users of the system appear to be satisfied with the functionality, dependability, and support of the GenTax application. Despite users' satisfaction with the system, our audit revealed that Technology Services and the Department of Finance can improve the security of the GenTax system in areas related to backup and storage, service account passwords, updating the network diagram, procedures related to adding, removing, and modifying user accounts, and managing insurance certifications.

Through stronger internal IT controls, the Department of Finance and Technology Services will be able to ensure that the GenTax application and data is more secure. Our report provides six recommendations to achieve this end.

This performance audit is authorized pursuant to the City and County of Denver Charter, Article V, Part 2, Section 1, *General Powers and Duties of Auditor*, and was conducted 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.

We extend appreciation to the Department of Finance, Technology Services and the personnel who assisted and cooperated with us during the audit.

Denver Auditor's Office

Timothy M. O'Brien, CPA
Auditor

REPORT HIGHLIGHTS

GenTax
April 2017

Objective

The objective of the audit was to determine the extent to which the GenTax application's administrative and systemic controls are designed to ensure data integrity and availability.

Background

In 2009 the City and County of Denver purchased and implemented GenTax, which is an integrated tax processing software package designed to support almost all aspects of excise tax collection. In 2015, collections through GenTax accounted for approximately $800 million of the City's revenue totals. The system is supported and administered by a third-party vendor, FAST Enterprises, which works as both the City's onsite and remote support team. GenTax is also supported by City employees who work in the Department of Finance, and the Technology Services department. These employees manage the hardware, maintenance, databases, and servers associated with GenTax to ensure system uptime and continuity.

Highlights

Our evaluation of the GenTax application found that users of the system are generally satisfied with the functionality and support of the application. However, improvements to the following areas are necessary to strengthen the security of the system.

- **Access to Backup and Storage**—A large number of Technology Services employees have unrestricted access to the backup and storage system associated with GenTax.
- **Service Accounts**—The majority of GenTax service account passwords have never been changed.
- **Architecture Drawing**—The network architecture diagram does not reflect the current GenTax infrastructure.
- **Access Control Process**—A documented process does not exist describing how employees are added to, removed from, or modified in the GenTax application.
- **Periodic Access Reviews**—A documented process does not exist for performing periodic access reviews.
- **Contract Compliance**—An updated insurance certificate was not being actively managed or monitored.

To enhance the existing IT controls surrounding the GenTax system, we offer six recommendations to the Department of Finance and Technology Services.

For a copy of this report visit, www.denvergov.org/auditor
Or contact the Auditor's Office at 720.913.5000

TABLE OF CONTENTS

BACKGROUND **1**

Overview of the Implementation of the GenTax System 1

OBJECTIVE **6**

SCOPE **6**

METHODOLOGY **6**

FINDING **8**

The Existing Information Technology Controls Surrounding the City's Tax Collection System Are Operating Effectively; However, Improvements Are Necessary to Further Secure the System and its Data 8

RECOMMENDATIONS **15**

AGENCY RESPONSE **16**

BACKGROUND

Overview of the Implementation of the GenTax System

The City and County of Denver (City) is experiencing one of the most prosperous times in history. With low unemployment rates, high job growth, and strong revenue inflows, the City truly supports its AAA bond rating.[1] This positive trend has yielded revenues totaling approximately $1.9 billion as recently as 2015 related to the City's governmental activities.[2] As the City continues to grow, effective management and operation of the technologies supporting the influx of City revenue will be of continued importance. GenTax is one of the City's technologies that supports the collection of approximately $800 million, representing 42 percent of the City governmental activity revenues. Figure 1 represents the tax types collected in 2015.

FIGURE 1. Types of Taxes Used to Collect Revenue through GenTax

Sales and Use ($640M)

- Sales tax - Tax on the purchase price paid or charged on retail sales, leases, or rentals of tangible personal property, and on certain services.
- Use tax - Consumer Use Tax on tangible personal property and taxable services that are used, stored or consumed within Denver. Retailer's Use Tax on manufacturers, vendors, or retailers who are located outside Denver but sell goods and services delivered into Denver.

Lodgers ($82M)

- Tax on the sale of lodging of 10.75%. The entire amount charged to any person for overnight accommodations or rooms for a duration of less than 30 days.

Occupational Privilege ($48M)

- Tax imposed on businesses (equaling $4.00 per month per employee) operating in the City and on individuals (equaling $5.75 per month per employee) who perform sufficient services within Denver to receive as compensation from an employer at least $500 for one calendar month.

Telecommunications ($2.7M)

- The Telecommunications business tax is a tax imposed at the rate of $1.12 per month for each of the telecommunications company's accounts within the City to which a basic dial-tone line is provided.

Facilities Development ($13M)

- A 10% facilities development admissions tax upon the purchase price of each admission to any entertainment, amusement, or athletic event or other production or assembly staged, produced, convened, or held in or on any City-owned or City-leased property. It is commonly referred to as the "seat tax."

Licenses ($439K)

- Fees collected by the City for the purposes of collecting and remitting tax payments. (Not reflected in the 2015 CAFR.)

Source: 2015 Comprehensive Annual Financial Report (CAFR)

[1] Often referred to as "Triple-A," this is the highest rating a financial institution assigns to issuers of bond debt. This indicates the strongest category of creditworthiness. This rating was assigned to the City's general obligation debt as of year-end 2015 by top credit rating agencies Standard & Poor's, Fitch Ratings Inc., and Moody's Investors Service.

[2] Governmental activities are basic services provided by the City, including police, fire, public works, sanitation, economic development, cultural events, and recreation. Sales, use, and property taxes finance the majority of these services.

In 2009, the City purchased and implemented GenTax, which is an integrated tax processing software package designed to support almost all aspects of tax collection. Streamlining the collection of six different tax types, GenTax has modernized the way the City conducts business.

GenTax replaced the City's previous tax system and was implemented in just under a year. GenTax was also implemented with a site license, which means that the system can be used by anyone with access in the City for tax collection-related work. A site license is generally less expensive because it allows for a large number of workers to access a system rather than purchasing a license for each individual user. Under the site license model, user access is limited to one location specified in the software license agreement.

GenTax Is a Commercial Off-the-Shelf System Administered by a Third Party

Unlike many of the technology systems used throughout the City, GenTax is a commercial off-the-shelf product that is fully developed, highly configurable, and ready to use upon purchase. This differs from internally developed software, which involves Technology Systems (TS) development, coding and testing of a system on behalf of a city agency. GenTax is also supported and administered by a third-party vendor, FAST Enterprises (FAST), which works as both the City's onsite and remote support team. FAST employees have responsibilities including facilitating the implementation of service patches, which include hot fixes, system upgrades, and new features and functionality. In addition, these support technicians can create, modify, and remove user accounts, or alter the actual code within GenTax.

The GenTax system is supported by FAST Enterprises, which provides an onsite and remote technical support team.

GenTax Use across the City

Like many software applications, GenTax has specific City employees who are responsible for managing various aspects of the system. These administrators work in the Technology Services department and the Treasury Division within the Department of Finance. These employees manage the hardware, maintenance, databases, and servers associated with GenTax to ensure system uptime and continuity.

Furthermore, the Department of Finance has subject matter experts (SMEs) who work closely with FAST personnel to handle the more complex functions such as training, upgrades to system features and functionality, patch implementation, user acceptance testing, and account maintenance. For example, FAST may roll out a change to GenTax that affects certain user capabilities within the system. The SMEs will work with FAST to test this change before it is implemented to ensure a smooth transition with little to no user interference.

GenTax Offers a Variety of User Functions

GenTax provides users with many different capabilities, including the ability to process customer payments, process tax returns, and monitor billing. Additionally, GenTax offers a robust audit feature that allows users of the system to create a history, or trail, which details information related to specific customers or cases. This feature enables other users to view and exchange information without having to exit the system.

Furthermore, GenTax offers a unique logging feature that captures snapshots of users' key strokes in real time. Users can replay these actions, which provides the ability to determine where errors

might have occurred during use. Additionally, the log can be used to provide step-by-step training to end users.

Many City Systems Interface with GenTax, Increasing Efficiency

GenTax interfaces with other City software systems, including the City's financial system, the eBiz tax center, and the Geographic Information System (GIS).[3] These interfaces act as a shared boundary in which elements of each system exchange information. For example, an end user may file business tax returns, make tax payments, or view the status of tax refunds using eBiz, which directly links to GenTax and eliminates the use of filing paper tax returns. In addition, GenTax may interface with GIS to establish a business address, which allows the City to properly split future tax revenues for the purposes of redeveloping a specific area of the City. When GIS is not used, or when the system cannot physically pinpoint a specific address, an address must be manually mapped to ensure that it is correctly assigned to the proper taxing district. Manual assignment is more time consuming and requires the approval of a SME who coordinates with other City employees to ensure accuracy.

GenTax System Security and Monitoring

Effective security and monitoring practices are an important element in ensuring the integrity and usability of data within any system, and protecting a system as vital as GenTax is a key aspect of the City's overall security posture. Monitoring the multitude of users, levels of access, and system interfaces is not a simple task for such a robust system, requiring the expertise of many members of the City's Technology Services department.

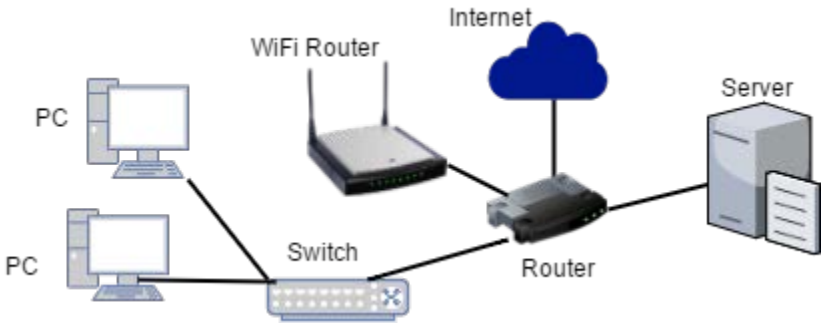
Currently, the City's Information Security Team monitors GenTax using QRadar, an integrated monitoring system that provides protection against threats and cybersecurity attacks.[4] Also known as a Security Incident and Event Monitor, this system logs Windows applications based on security rules. For example, if there are several invalid login attempts to a GenTax user account, QRadar will send an alert to an appropriate member of the Information Security Team. Technology Services also monitors the GenTax system for availability and disk space.

Finally, Technology Services uses a system architecture diagram of GenTax, which provides conceptual models that define an overall view of a system and outlines relationships to the system and its various shared interfaces. A network diagram may include hundreds of different icons that represent devices such as a PC, a complex server, or cloud-based storage system. This type of diagram is also useful when trying to track down problems with a system. For example, when troubleshooting a system, a system administrator needs to have an up-to-date depiction of the various devices connected to the system. This allows the administrator to pinpoint where a problem is occurring and identify a root cause. Without an accurate diagram, an administrator might not even know a certain PC or device is connected to the network, which could be the cause of an issue. Figure 2 provides a simplified example of an architectural diagram.

[3] eBiz is a taxpayer access portal that offers a friendly user interface for business to file returns, make payments via electronic check or credit card, and manage tax accounts.

[4] QRadar collects data from GenTax and from its various network devices and then monitors for vulnerabilities and inappropriate user activity behavior.

FIGURE 2. System Architecture Diagram Example



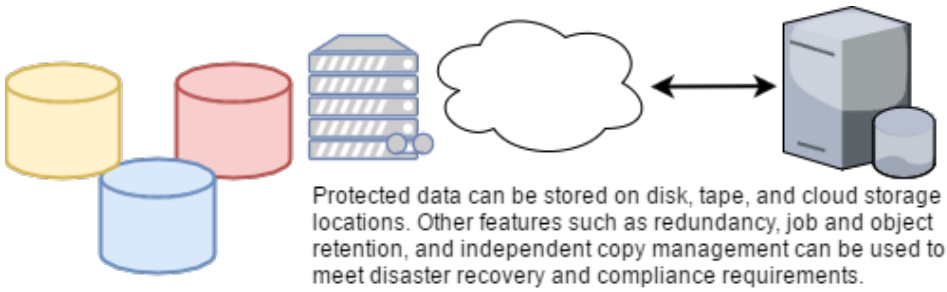
Source: Created by the Audit Services Division.

GenTax Backup and Storage

Another element of ensuring system security involves backup and storage. In the event of a system failure or a disaster, it is important that the City be able to restore any lost data or information within GenTax in a timely fashion. For this reason, the City uses a software system called CommVault to perform backup and restores of GenTax data as needed.

CommVault provides protection for data through the use of software on physical or virtual hosts.[5] Database administrators use CommVault to monitor backup schedules and modify or plan when a backup of the system should be performed. All activity is tracked in a centralized location and is managed by administrators through a central user interface. Backed up data is replicated and stored in a fashion that abides by City policy to mitigate potential data loss in the event of a disaster. Figure 3 provides a graphical representation of some of the more common storage options used for systems such as GenTax.

FIGURE 3. Data Storage Options



Source: Created by the Audit Services Division.

[5] Virtual hosting or housing is a method of hosting which enables a server to share its resources, such as processor load, or memory, which allows for faster performance.

Change Management Processes

The practice of change management related to GenTax can be compared metaphorically to the use of traffic lights at intersections. The purpose of traffic lights is to control the flow of motor vehicle traffic and to help pedestrians safely cross intersections. Similarly, change management is used to control system and application changes as they flow through process sequences. Without traffic lights, collisions are bound to occur. Similarly, if changes are introduced with uncontrolled process sequences, disruptions to GenTax services are highly likely.

> Change management controls the flow of system and application changes to minimize GenTax service disruptions.

GenTax follows a very structured change management process that includes many different levels of decisions and analysis. This process includes the involvement of SMEs, FAST personnel, Technology Services, and many others. These individuals work to develop, test, stage, and eventually implement changes to the live environment known as *production*. For example, with the addition of marijuana taxation, GenTax needed to be configured to include medical and recreational marijuana sales tax. Before this change was implemented in the production system, it was configured, approved, and tested by users and management.

OBJECTIVE

The audit objective was to determine the extent to which the GenTax application's administrative and systemic controls are designed to ensure data integrity and availability.

SCOPE

The audit focused on system controls that are in place within and surrounding the GenTax application. Specifically, the audit reviewed access controls, change management, security and monitoring, and backup and recovery for multiple environments including the GenTax production application and database servers. In addition, the audit included a review of the FAST Enterprises vendor contract for compliance with contract terms.

The audit did not examine payment/return processing through the taxpayer access portal (eBiz). Payments transacted through eBiz are processed through a separate interface, Enterprise Cashiering System, which is evaluated during the annual Payment Card Industry audit. Additionally, operational segregation of duties was scoped out of this audit based on testing previously conducted during the 2016 Municipal Sales Tax Collection Practices Audit.

METHODOLOGY

We applied various methodologies during the audit process to gather and analyze information pertinent to the audit scope, and to assist with developing and testing the audit objectives. The methodologies included the following:

- Conducting interviews with key personnel to obtain an understanding of the GenTax operating environment, and to assess the presence of administrative and application controls
- Evaluating the design and operating effectiveness of administrative and application controls that are relevant to the audit objectives
- Reviewing the user account creation, modification, and termination process
- Determining whether access control actions are conducted based on documented procedures
- Reviewing network procedures for authenticating to the GenTax application, including capturing screenshots to determine whether password complexity and requirements meet Technology Services standards
- Reviewing the frequency of service-account password changes for GenTax application and related databases
- Determining whether subject matter experts perform access reviews to ensure that system access is appropriate based on job responsibilities
- Obtaining documented policies and procedures for the change management process, as well as reviewing a listing of changes that occurred in 2016 from the database system to determine whether changes are tracked, approved, and tested prior to implementation

- Obtaining screen shots of the GenTax backup schedule to ensure that the application and databases are regularly backed up
- Reviewing recovery testing to determine whether data and application backups are recoverable and whether data is complete and accurate
- Reviewing users with access to the CommVault back-up and storage system to determine appropriateness of access based on job responsibilities
- Obtaining screen shots showing evidence of monitoring the application and databases for security incidents, data integrity, and availability
- Obtaining and reviewing copies of the contracts and amendments between software provider FAST Enterprises and the City and County of Denver regarding the GenTax system
- Determining whether FAST Enterprises has a report pertaining to GenTax security, confidentiality/privacy, or processing integrity controls at a service organization
- Interviewing FAST Enterprises Information Technology Director and Manager to understand relevant company practices, including security awareness training, secure coding practices, periodic penetration testing, and compliance audits[6]
- Reviewing FAST Enterprises contract for insurance coverage and obtaining proof of current insurance coverage

[6] "What is Penetration Testing," Penetration testing is an attempt to evaluate the security of an IT infrastructure by safely trying to exploit vulnerabilities, accessed March 16, 2017 https://www.coresecurity.com/penetration-testing-overview.

FINDING

The Existing Information Technology Controls Surrounding the City's Tax Collection System Are Operating Effectively; However, Improvements Are Necessary to Further Secure the System and its Data

In assessing the City's tax collection system, GenTax, we found some assurance as well as some areas for improvement. Based on interviews and feedback, users of the system appear to be satisfied with the functionality, dependability, and support of the GenTax application. From an external user perspective, GenTax appears to provide a convenient way for businesses to pay taxes and offer an easy user interface to these and other end users. However, the audit team identified three areas where Technology Services (TS) and the Department of Finance can further enhance the system. First, we found that Technology Services can improve security surrounding access to the backup and storage of tax data as well as service account passwords and updating the network diagram. Second, the Department of Finance could develop procedures related to adding, removing, and modifying user accounts. Third, we found that Technology Services could provide additional due diligence in managing and monitoring GenTax-related contracts. By addressing these areas, Technology Services and the Department of Finance will enhance the security of the GenTax system and its data.

GenTax Provides Functionality and Support for Users

GenTax offers internal users the ability to perform tax administration activities for multiple tax types, including payment processing, delinquent tax collection, monitoring, auditing, document retention, and reporting. For example, internal GenTax users can generate a collections letter to notify a taxpayer of a delinquent remittance, storing the letter within the system for record-keeping purposes. This type of functionality facilitates robust case management.

From the perspective of an external user, businesses use GenTax to manage their taxes through a web portal that is linked to the GenTax system. This feature allows businesses to pay, monitor, and provide feedback in real-time. During the audit, the team received numerous confirmations that the system meets the needs of both internal and external users.

We determined that the success of the system is contributable to several factors, as follows:

- **Knowledge Support** – The third-party vendor, FAST Enterprises (FAST), has trained technical staff working on site for the City. Additionally, there are subject matter experts (SMEs) within the Department of Finance whose roles include supporting GenTax users.
- **Responsiveness** – Technology Services maintains the application and database servers for increased response to technical issues encountered by users.
- **Monitoring** – The GenTax system and databases are monitored in three areas to ensure confidentiality, integrity, and availability.
- **Testing** – Any changes to the GenTax system or database are fully tested prior to being implemented, which decreases the risk of the system being unavailable.
- **Logging Feature** – The GenTax application has a unique logging feature that captures users' key strokes. When problems arise, this feature can be used to determine where errors might have occurred that contributed to the problem. Additionally, the log can be used to provide step- by-step training to end users.

Despite the assurance we obtained regarding the GenTax system, we also identified three opportunities for improvement in the area of security.

Technology Services Can Strengthen the Security Posture of the GenTax System

In the Information Technology security space, there are several key operational activities that provide a foundation for overall system security. While reviewing the internal controls related to the GenTax system and database security, the audit team identified three security categories that need to be strengthened. The first relates to system access, the second relates to the management of service accounts, and the third relates to the architecture diagram.

Several Employees Have Unrestricted Access to a Critical System That Is Used Citywide for Backup and Storage of Applications and Databases

During a review of the users who have access to the CommVault data protection system, the audit team discovered more than 100 accounts with varying levels of access to the GenTax backup system. However, we verified that the Technology Services team that administers CommVault is significantly smaller than 100, consisting of only 11 system administrators. No formal review process is in place by which to periodically assess the accounts and privileges that can access the CommVault application.

In the absence of a process for reviewing user accounts and associated privilege levels, the potential exists that a separated employee, or an employee that changes departments and retains access could put the system at risk by intentionally or unintentionally disrupting, deleting, or corrupting highly sensitive or important City data. Section AC-3.1 of the Federal Information System Controls Audit Manual (FISCAM) provides relevant guidance for this situation, recommending that resource owners identify authorized users and the appropriate access level. These resource owners should perform periodic access reviews to verify that access continues to be warranted based on a valid business purpose.

RECOMMENDATION 1.1

The Chief Information Officer should ensure that Technology Services performs a review and clean-up of user accounts with access to CommVault. Additionally, Technology Services should create a process for ongoing periodic access reviews for the CommVault system.

Agency Response: Agree, Implementation Date – October 1, 2017

Service Accounts Not Tied to Individual Accounts

The GenTax system has 10 service accounts that are used for certain administrative procedures. These accounts can be machine-based accounts, which are used to communicate from machine to machine when different systems need to interface. Alternatively, service-based accounts are used to run a service, such as system maintenance tasks. A review of the last password change date for these accounts revealed that only 1 of the 10 service account passwords has been changed since GenTax and the taxpayer access portal module (eBiz) were implemented in 2009 and 2012, respectively.

> Only 1 of the 10 service account passwords has been changed since GenTax and eBiz were implemented in 2009 and 2012, respectively.

Since service and machine-based accounts work within a system rather than by individual users, they may have associated account or password settings that differ from individual user account settings. For example, service accounts may have longer password lengths or an exception from forced automated password changes that might cause an unplanned system outage. Although these account passwords may not expire on an automated basis, standards such as National Institute of Standards and Technology (NIST) 800-53 IA-5 suggest that an organization should establish and enforce a maximum password lifetime for any system using password-based authentication, not just for individual user accounts. The Windows Server 2008 R2 Security Technical Implementation Guide provides specific policy guidance for service account passwords.[7] A policy governing this process should state that manually generated application account passwords that are "entered by a system administrator are changed at least annually or when a system administrator with knowledge of the password leaves the organization."[8]

Technology Services has not established a policy regarding service account user and password security settings. In addition, there is no process or procedure for managing service account password changes.

Service accounts typically have privileged level access to databases and applications and their passwords are infrequently or never changed. Therefore, these accounts could be compromised to gain unauthorized access to a system. Technology Services has instituted monitoring and alerting protocols for failed login attempts; however, the audit team recommends that Technology Services needs to take further action to protect these powerful accounts.

[7] The Windows Server 2008 R2 Member Server Security Technical Implementation Guide was developed based on Microsoft Corporation security templates and Department of Defense consensus.

[8] "Windows Server 2008 R2 Member Server Security Technical Implementation Guide," accessed February 23, 2017, https://www.stigviewer.com/stig/windows_server_2008_r2_member_server/2014-04-02/finding/V-14271.

RECOMMENDATION 1.2

The Chief Information Officer should work with FAST Enterprises to develop a documented service account policy that specifies a detailed description of each service account, what it interfaces with, who the owner is, and includes password length and change requirements. Additionally, Technology Services should work with FAST Enterprises to change the initial service account passwords.

Agency Response: Agree, Implementation Date – October 1, 2017

GenTax Architecture Diagram Not Accurate

During audit work, we reviewed the GenTax system architecture diagram because of its importance in assisting the technical team with understanding how devices are placed, connected, and engineered to form a complete picture of the network. During this assessment, we discovered that the GenTax architecture diagram is out of date and does not accurately reflect the current network environment. We determined the network environment has changed since the system was implemented. Specifically, additional hardware devices are in place, such as load balancers, which distribute network traffic and increase the reliability of applications. Additionally, an intrusion prevention system has been added to the existing environment for monitoring and securing the GenTax system and databases. However, the current network diagram does not reflect the updated network environment. We determined that the diagram is outdated because Technology Services does not have a protocol in place for updating the diagrams when a change to the network or system's overall architecture is made.

> The GenTax architecture diagram does not accurately reflect the current network environment.

An accurate network diagram is necessary for understanding how the GenTax application and databases are physically connected. Moreover, it is a valuable resource for troubleshooting issues. Further, a diagram is essential for ensuring that the system is configured to prevent future compromises or security threats. As NIST 800-53 revision 4 specifies, an organization should develop, document, and maintain under configuration control a current baseline configuration of any information system. The baseline configuration should reflect the current enterprise architecture.

RECOMMENDATION 1.3

The Chief Information Officer should work with FAST Enterprises to ensure that system architecture drawings are complete and accurate, and are kept up to date.

Agency Response: Agree, Implementation Date – October 1, 2017

Department of Finance Needs to Develop Procedures Related to Adding, Removing, and Modifying User Accounts

In addition to the issues we identified surrounding the security posture of the GenTax system, we noted opportunities to more formally establish and document procedures to manage user accounts. The Department of Finance has more than 100 GenTax user accounts that are used to perform various functions, such as handling sales tax payments, returns, refunds, transactions, and other types of tax transactions. User accounts are added for new employees and removed when employees retire, transfer positions, or no longer require access. These additions and removals are handled by subject matter experts (SMEs) in the Department of Finance who contact FAST support personnel to add or modify account access. However, we found that this request process is informal in nature. Further, the method of communication appears to be inconsistent; sometimes requests are communicated in person or emailed. At other times, requests are submitted through an automated ticketing mechanism. When auditors inquired as to the City's official method, we were informed that a formal process has never been established or documented. Additionally, we were informed that SMEs are not performing periodic access reviews of the access rights associated with these user accounts.

NIST provides guidance on the importance of documenting processes, which is instructive in this situation. NIST Special Publication 800-53 revision 4 specifies that organizations should develop, document, and disseminate an access control policy. This policy should include a process for adding and removing user accounts. Additionally, to adequately control user accounts, access reviews should be periodically performed to determine whether accounts remain accurate.

GenTax comprises much of the City's revenue and is extremely important for accurately recording sales and use tax. Without a documented process in place, employees responsible for adding and removing user accounts may not be fully aware of their responsibilities. This could result in unauthorized individuals who retain access to GenTax, which could allow those individuals to modify sales and use tax payments.

RECOMMENDATION 1.4

The City Treasurer should develop, document, and disseminate an access control policy that includes a process for adding and removing user accounts for the GenTax application.

Agency Response: Agree, Implementation Date – April 30, 2017

RECOMMENDATION 1.5

The City Treasurer should establish develop, document, and disseminate a policy for periodic access reviews.

Agency Response: Agree, Implementation Date – April 30, 2017

Technology Services Inadequately Manages the GenTax Insurance Requirements Under the Software Contract

The final area we found for improvement in the City's administration of the GenTax system is related to the system's insurance certification. The contract between the City and FAST for the GenTax system specifies the types and amounts of insurance that the vendor needs to maintain during the term of the agreement and for a period of three years following the termination of the agreement. The insurance coverage provided includes commercial general liability, workers' compensation, and professional liability. The ACORD certificate provided with the 2012 contract amendment evidenced insurance coverage through January 1, 2013, for most required insurance types except professional liability coverage which was extended through January 1, 2015.[9,10] We requested an updated ACORD certificate for review, Technology Services (TS) could not produce one and did not have any knowledge of a current insurance certification for FAST Enterprises.

> Technology Services is not effectively monitoring the FAST Enterprises contract for insurance coverage. We previously made a recommendation to Technology Services to enhance its contract monitoring procedures in a 2015 audit.

During the audit we contacted FAST personnel who provided an updated insurance certificate. Technology Services should be performing this task in accordance with official City policy. Executive Order 8 specifies that the initiating authority for a contract—which, in this case, would be Technology Services—is responsible for ensuring that contract provisions continue to be met. For example, Technology Services should be monitoring the insurance coverage retained by the vendor that provides on-site maintenance and support for GenTax for continuous compliance, as well as monitor policy effective dates to ensure that they are current.

It is important to note that this is a repeat finding from our 2015 audit of the IT Service Desk. Auditors found that Technology Services did not have current insurance certification documentation for a vendor providing outsourced service desk support. In response to our related audit recommendation, Technology Services agreed to establish a process to periodically review the contract between the IT Service Desk and the third-party vendor for continued compliance with contractual terms, including verifying that the vendor is maintaining insurance coverage. Accordingly, Technology Services hired a contract administrator to allow for more effective contract control. However, this is a relatively new position within the organization and, as such, key personnel are still in the processes of learning all related contract logistics. Therefore, TS was not aware of all responsibilities associated with maintaining this contract.

Current insurance certificates are required to verify that vendors maintain insurance in the types and amounts specified by the contract. The insurance provisions in City contracts provide coverage to the City should an event occur that would be covered under insurance, such as a data breech. Without adequate insurance coverage the vendor might not have the resources to cover the liability incurred. This could result in negotiations or legal actions in order to meet any obligations.

[9]ACORD (Association for Cooperative Operations Research and Development) is a global nonprofit association working to improve data quality for the insurance industry. https://www.acord.org/about/pages/default.aspx.
[10] An ACORD form is an insurance industry standardized form.

RECOMMENDATION 1.6

The Chief Information Officer should ensure that Technology Services monitors the GenTax contract for compliance and ensures that the City receives updated insurance certificates annually or based on upon the insurance term provided.

Agency Response: Agree, Implementation Date – October 1, 2017

RECOMMENDATIONS

1.1 **Review and Clean-up User Accounts**— The Chief Information Officer should ensure that Technology Services performs a review and clean-up of user accounts with access to CommVault. Additionally, Technology Services should create a process for ongoing periodic access reviews for the CommVault system.

Auditee Response: Agree, Implementation Date – October 1, 2017

Auditee Narrative: Technology Services will develop a process to periodically review access to CommVault to ensure access is limited to only necessary accounts.

1.2 **Develop a Documented Service Account Policy**— The Chief Information Officer should work with FAST Enterprises to develop a documented service account policy that specifies a detailed description of each service account, what it interfaces with, who the owner is, and includes password length and change requirements. Additionally, Technology Services should work with FAST Enterprises to change the initial service account passwords.

Auditee Response: Agree, Implementation Date – October 1, 2017

Auditee Narrative: Technology Services will formalize a service account policy and work with FAST Enterprises to address account description, interfaces, owners, and password length and change requirements including the reset of initial passwords.

1.3 **Update System Architecture Drawings**— The Chief Information Officer should work with FAST Enterprises to ensure system architecture drawings are complete and accurate, and kept up to date.

Auditee Response: Agree, Implementation Date – October 1, 2017

Auditee Narrative: Technology Services will work with FAST Enterprises to ensure system architecture diagrams are complete and accurate, and kept up to date.

1.4 **Develop a Policy for Adding, Modifying, and Removing User Accounts**— The City Treasurer should develop, document, and disseminate an access control policy that includes a process for adding, modifying, and removing user accounts for the GenTax application.

Auditee Response: Agree, Implementation Date – April 30, 2017

Auditee Narrative: The Department of Finance agrees with this recommendation. A formal policy regarding access control to GenTax will be written and incorporated into the new "on- and offboarding" process that will be included in the duties of the newly hired Office Administrator in DOF.

1.5 **Develop an Access Review Policy**— The City Treasurer should establish develop, document, and disseminate a policy for periodic access reviews.

Auditee Response: Agree, Implementation Date – April 30, 2017

Auditee Narrative: Once the Audit Team identified this issue during the audit, Treasury performed a full review of the GenTax database users and identified those that no longer required access or needed their access changed due to change in job functions. This user database cleanup was completed in February and will be reviewed twice a year going forward. A formal written policy documenting this procedure will be completed.

1.6 **Improve Contract Monitoring**— The Chief Information Officer should ensure that Technology Services monitors the GenTax contract for insurance compliance and ensures that the City receives updated insurance certificates annually or based on upon the insurance term provided.

Auditee Response: Agree, Implementation Date – October 1, 2017

Auditee Narrative: Technology Services will adopt a process to ensure our GenTax vendor provides ongoing proof of insurance coverage in compliance with our contract terms.

AGENCY RESPONSE

DENVER
TECHNOLOGY SERVICES

Technology Services
201 West Colfax Avenue
Department 301
Denver, CO 80202

April 11, 2017

Auditor Timothy O'Brien, CPA
Office of the Auditor
City and County of Denver
201 West Colfax Avenue, Dept. 705
Denver, Colorado 80202

Dear Mr. O'Brien,

The Office of the Auditor has conducted a performance audit of GenTax.

This memorandum provides a written response for each reportable condition noted in the Auditor's Report final draft that was sent to us on March 21, 2017. This response complies with Section 20-276 (c) of the Denver Revised Municipal Code (D.R.M.C.).

AUDIT FINDING 1
The existing IT controls surrounding the City's Tax Collection System are operating effectively, however opportunities exist to further secure the system and its data.

RECOMMENDATION 1.1
The Chief Information Officer should ensure that Technology Services performs a review and clean-up of user accounts with access to CommVault. Additionally, Technology Services should create a process for ongoing periodic access reviews for the CommVault system.

Agree or Disagree with Recommendation	Target date to complete implementation activities (Generally expected within 60 to 90 days)	Name and phone number of specific point of contact for implementation
Agree	October 1, 2017	Jeff Johnson 720-913-5810

Narrative for Recommendation 1.1
Technology Services will develop a process to periodically review access to CommVault to ensure access is limited to only necessary accounts.

RECOMMENDATION 1.2 The Chief Information Officer should work with FAST Enterprises to develop a documented service account policy that specifies a detailed description of each service account, what it interfaces with, who the owner is, and includes password length and change requirements. Additionally, Technology Services should work with FAST Enterprises to change the initial service account passwords.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and phone number of specific point of contact for implementation**
Agree	October 1, 2017	Tricia R. Scherer 720-913-4869

Narrative for Recommendation 1.2
Technology Services will formalize a service account policy and work with FAST Enterprises to address account description, interfaces, owners, and password length and change requirements including the reset of initial passwords.

RECOMMENDATION 1.3 The Chief Information Officer should work with FAST Enterprises to ensure system architecture drawings are complete and accurate, and kept up to date.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and phone number of specific point of contact for implementation**
Agree	October 1, 2017	Michael Wright 720-913-4864

Narrative for Recommendation 1.3
Technology Services will work with FAST Enterprises to ensure system architecture diagrams are complete and accurate, and kept up to date.

RECOMMENDATION 1.4 The City Treasurer should develop, document, and disseminate an access control policy that includes a process for adding, modifying, and removing user accounts for the GenTax application.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and phone number of specific point of contact for implementation**
Agree	April 30, 2017	Judy Bonato, Operations Manager 720-913-9319

Narrative for Recommendation 1.4
The Department of Finance agrees with this recommendation. A formal policy regarding access control to GenTax will be written and incorporated into the new "on- and off-boarding" process that will be included in the duties of the newly hired Office Administrator in DOF.

RECOMMENDATION 1.5 The City Treasurer should establish develop, document, and disseminate a policy for periodic access reviews.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and phone number of specific point of contact for implementation**
Agree	April 30, 2017	Judy Bonato, Operations Manager 720-913-9319

Narrative for Recommendation 1.5
Once the Audit Team identified this issue during the audit, Treasury performed a full review of the GenTax database users and identified those that no longer required access or needed their access changed due to change in job functions. This user database clean-up was completed in February and will be reviewed twice a year going forward. A formal written policy documenting this procedure will be completed.

RECOMMENDATION 1.6 The Chief Information Officer should ensure that Technology Services monitors the GenTax contract for insurance compliance and ensures that the City receives updated insurance certificates annually or based on upon the insurance term provided.		
Agree or Disagree with Recommendation	**Target date to complete implementation activities (Generally expected within 60 to 90 days)**	**Name and phone number of specific point of contact for implementation**
Agree	October 1, 2017	Chad Mitchell 720-913-2642

Narrative for Recommendation 1.6
Technology Services will adopt a process to ensure our GenTax vendor provides ongoing proof of insurance coverage in compliance with our contract terms.

Please contact Stephen E. Coury at 720-913-4919 with any questions.

Sincerely,

Steve Ellington
Treasurer

Scott Cardenas
Chief Information Officer

cc: Valerie Walling, Deputy Auditor, CPA,CMC
Dawn Wiseman, Audit Manager, CRMA
Shannon Kuhn, Information Technology Audit Supervisor, CISA
Christine Binnicker, Deputy Chief Information Officer
Chris Todd, Chief Technology Officer