

City Auditor's Office *Hosted Applications Audit*

September 2020



City Auditor, Lori Brooks Jaquess, CPA, CIA, CGAP, CRMA
Assistant City Auditor, Susan Edwards, CIA, CFE
Information Technology Auditor, Roshan Jayawardene, CISA

NOTE: This version of the Hosted Applications Audit Report has been redacted by the City Attorney's Office to remove confidential information that, if publicly released, could compromise the security of City assets.





City Auditor's Office

September 24, 2020

Honorable Mayor and Members of the City Council:

The City Auditor's Office has completed the Hosted Applications Audit. The purpose of the audit was to review internal controls in Citywide hosted applications.

Management's response to our audit findings and recommendations, as well as target implementation dates and responsibility, is included following the report.

We would like to thank staff from the Information Technology department and other departments' information technology staff for their full cooperation and assistance during the audit.

Lori Brooks Jaquess

Lori Brooks Jaquess, CPA, CIA, CGAP, CRMA
City Auditor

Attachment

cc: Trey Yelverton, City Manager
Jim Parajon, Deputy City Manager
Gilbert Perales, Deputy City Manager
Jennifer Wichmann, Assistant City Manager
Enrique Martinez, Chief Information Officer
Mike Finley, Chief Financial Officer

Table of Contents

| | <u>Page</u> |
|---|-------------|
| Executive Summary | 1 |
| Audit Scope and Methodology | 2 |
| Background | 4 |
| Audit Results..... | 8 |
| Detailed Audit Findings..... | 10 |
| Audit Recommendation and Response Table | 24 |
| Appendix A | 28 |
| Appendix B..... | 29 |

Executive Summary

The City Auditor's Office has completed the Hosted Applications Audit. The performance audit 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 objective. The audit objective was to review and evaluate current internal controls related to the use of hosted software solutions.

The City Auditor's Office noted the following strengths related to hosted solutions:

- Better internal controls are present with hosted applications vetted through the IT (Information Technology) governance process
- The need to maintain software internally is reduced
- Cost reduction is a possibility

We noted the following potential opportunities for improvement:

- Amending the IT governance process to include additional hosted software applications
- Obtaining vendor commitments for improved data center internal controls in Budget and Parks software applications
- Limiting vendor master file changes in Lawson to City personnel
- Improving controls in Water department social media
- Using software performance monitoring tools

Details of audit findings, conclusions and recommendations are included in the following report.

Audit Scope and Methodology

The objective of the audit was to review and evaluate current internal controls related to the use of hosted software solutions. Hosted software includes applications used by many City departments, where users log into the software at a vendor-controlled site via the internet. The data and transactions are stored at the vendor owned site, outside of City owned premises. Our review process included an inventory of all hosted applications used Citywide and selection of a detailed sample of 30, based on data value and risk. The review process was focused on key risk areas, such as data security, backup and recovery, contractual clauses to protect the City, and compliance with common hosted applications standards established by the American Institute of Certified Public Accountants (AICPA).

To adequately address the audit objectives and to describe the scope of work on internal controls, the following methodology was used in completing the audit:

- Obtained a list of applications used Citywide and interviewed staff in each department to identify and validate the inventory of hosted solutions
- Communicated with vendors included in the audit sample to obtain necessary documentation and feedback
- Reviewed control and compliance documents for the selected hosted applications
- Conducted research on hosted application risks, controls, and trends in cloud technology solutions
- Reviewed contract related clauses with the City Attorney's Office

The audit was conducted in accordance with generally accepted government auditing standards. These standards require that we determine whether internal controls are significant to the audit objective. If internal controls are significant to the audit objective, the standards require that the auditor obtain an understanding of the controls. In understanding and evaluating internal controls, the City Auditor's Office adheres to the Committee of Sponsoring Organizations of the Treadway Commission's Internal Control – Integrated Framework (COSO Framework) as included in Standards for Internal Control in the Federal Government (Green Book).

According to the COSO Framework, internal control is a process effected by an entity's oversight body, management, and other personnel that provides reasonable assurance that the objectives of an entity will be achieved. These objectives and related risks can be broadly classified into one or more of the following three categories: (1) Operations - effectiveness and efficiency of operations; (2) Reporting - reliability of reporting for internal and external use; and (3) Compliance - compliance with applicable laws and regulations.

Hosted Applications Audit

In planning and performing the audit, we obtained an understanding of related internal controls and assessed the internal control risks significant to our audit objective. We determined the following internal control components were significant to our audit objective:

- Control Environment - The overall data and cloud environment under vendor control
- Risk Assessment - Continuous assessment of risk to the data and cloud environment
- Control Activities - Adherence to accepted control and compliance standards and contractual safeguards to the City
- Monitoring - Continuous monitoring of the data and cloud environment for adverse activity per AICPA standards
- Information and Communication - Updates, application feedback and keeping the City informed on operational matters

The deficiencies in internal control, which are significant within the context of the audit objective and based upon the audit work performed, are stated in the Detailed Audit Findings section starting on page 10.

For further information regarding internal control components and the related principles of internal control, please see Appendix A.

Background

The technology trend of using hosted and cloud services began more than a decade ago. The City of Arlington began contracting for hosted solutions around 2009, with the new Handitran bus ride scheduling software. The City had been using hosted applications, related to financial and governmental institutions (i.e. Chase, Bank American, State of Texas) even prior to that time. The number of hosted applications has been steadily increasing since that time. There are currently about 195 hosted applications used Citywide, shown in Appendix B.

The basic concept of a hosted application is that the City enters into an agreement with a software vendor. The vendor agrees to provide a web-based solution, where the users access a website controlled by the vendor to enter transactions. The vendor retains the data at their own facility or at a rented 3rd party location, which is referred to as the Cloud, on behalf of the City. The vendor maintains the application software and the necessary security environment to protect the data, including backup and recovery in the event of disruption of services.

Software vendors are increasingly using Cloud sites to transact and store data due to low cost. Common Cloud site vendors include Amazon Web Services (AWS), Microsoft Azure and Rackspace, to name a few. At cloud sites, such as AWS, software vendors are given a physical building with security, all the hardware needed to transact and store data, a security apparatus with defenses against cyber threats, and backup and recovery services. The cost of cloud computing is decreasing at a steady pace, resulting in the economic advantage of using cloud sites by many software vendors. The City's main responsibility in using a hosted solution is to provide a secure, reliable connection to the internet.

Another type of hosted solution is a colocation center. Colocation centers provide a physical building with security, an internet connection, and power supply for vendors to rent. The vendors are responsible for setting up their own equipment at colocation sites, maintaining the application, and providing cyber security and backup and recovery for their individual customers. The colocation option is cost effective to software vendors since the need to own and maintain a physical building and real estate is eliminated. Traditional Cloud sites, as well as vendor sites at Colocation centers, follow a virtualized computer environment model, where an array of hosts and virtualized computers offer services to clients.

Types of hosted application methods used by the City include:

- Contractual agreement with a software vendor where the data is stored at the vendor's own data center or at a Cloud site.
- Contractual agreement with an entity, such as a bank or other financial institution, allowing entry of information to a City owned account, which can be classified as a "log in" system. The data is in the custody of the vendor. The City can run reports, and some data is transferred to a City owned application, such as Lawson.

Hosted Applications Audit

- A State or Federal Government website (e.g. Social Security Administration, Texas Attorney General) where there is no specific agreement; however, laws and regulations require the City to enter data to these systems. Data is under the control of the specific agency.
- Various credit card processors for City applications, where payment data is at a vendor site and then transferred to the City's financial system. These are bound by payment card industry (PCI) compliance standards for data security and storage

The American Institute of Certified Public Accountants (AICPA) has established data security and control standards for hosted environments. The standards require cloud providers and vendors providing hosted services to follow strict criteria for data security, cyber security and other criteria aimed at protecting client data and transaction integrity. These guidelines are listed as Standards for Attestation Engagements (SSAE) 16, an auditing standard for service organizations. The SSAE16 guidelines consist of three compliance standards, referred to as Service Organization Controls (SOC) 1, 2 or 3. Service providers are audited by an independent qualified third-party assessor for the three criteria. Each is explained below.

- **SOC1** - Review process to assess internal controls over financial reporting
- **SOC2** - Review process to assess controls in a service organization and includes auditor testing and results
- **SOC3** - Review process that provides a service organization description and auditor opinion in a condensed document

One of the audit objectives was to review the SOC2 document for the sites where Arlington data resides. We reviewed the SOC2 document because it provides evidence of an independent assessment and testing of the data center control environment. Most of Arlington's data is public record; however, some sensitive data, particularly in public safety, Human Resources (HR) and Finance applications are stored in hosted environments. Both data types must be safeguarded to a degree that would enable the City to operate with minimal interruptions, protect from intrusion, and safeguard the integrity of transactions. The SOC2 assessment criteria include the following:

Data Privacy - Access control, authentication, and encryption

Data Security - Network, application firewalls, authentication, and intrusion detection

Data Availability - Performance monitoring, disaster recovery, and security incident handling

Data Processing Integrity - Quality assurance and process monitoring

Data Confidentiality - Encryption, access controls, network and application firewalls

Hosted Applications Audit

Risks the City may encounter with hosted applications are not limited to controls at the site where the data resides. A vendor contract or service agreement favorable to City operations is also necessary. A contract or a service agreement lists clauses, service standards, service delivery and other service-related parameters the City would be provided while using the software. Vendors usually agree to a customized contract or service agreement when implementing large scale software projects. Smaller scale software hosted solutions consist of a service agreement that is standard to anyone using the product. These are usually favorable to the vendor, providing the bare minimum of services for a fee, while customizations favorable to the user may be allowed for a higher fee. Some service agreements are not negotiable. Key aspects of a hosting contract or service agreement beneficial to the City are listed below:

- **Software performance standards** - A vendor guarantee that software will be available to users and free of errors, stated as a percentage of time.
- **Exit strategy** - A vendor guarantee that City data and transaction history will be provided in a usable format to the City, within a specific time period after the vendor relationship ends and the software use is discontinued.
- **City Indemnification** - A vendor guarantee that the City of Arlington will be indemnified for errors or exposures of City transactional data. The City, the owner of the data, can be held liable for errors and unauthorized data exposures, such as cyber related hacking.
- **Incident response times** - A vendor guarantee that error related work orders will be rectified based on a priority level and within specific time frames.
- **Patch management** - A vendor guarantee that application software will be updated as necessary in a timely manner. Vendors are responsible to maintain software regardless of whether it is at a Cloud site or Colocation site.
- **Security controls** - A vendor commitment to secure City data with access control methods, audit trails, and security upgrades to application software.
- **Compliance requirements** - A vendor commitment to safeguard data, due to compliance requirements such as Health Insurance Portability and Accountability Act (HIPAA) or public safety Criminal Justice Information Security (CJIS) requirements.
- **Backup and recovery** - A vendor commitment for recovery of software functionality after a disaster or other disruptive event within a specific timeframe.
- **Cyber Security** - A vendor commitment to maintain insurance coverage for Cyber related security incidents and data exposure.

Hosted Applications Audit

IT Governance Process

The City currently follows an IT governance process, which was established in 2013. It requires departments seeking technology solutions to submit software implementation projects to the Information Technology (IT) department for review. Generally, projects expected to have a cost of more than \$50,000 or require more than 80 hours of IT staff time are subject to the governance process. The projects are then submitted to the City Manager's Office for approval. Approval is based on funding availability and the City's ability to accommodate the solution within the existing technology infrastructure and staffing levels.

IT department oversight of the project includes project management, infrastructure needs, security setup, vendor selection, vendor negotiations and software testing to name a few. The governance process is also tied to procurement procedures, which require obtaining bids and a request for proposals (RFP) document that contains standard baseline requirements, such as liability insurance, certain compliance needs, and the specifications of the software itself.

Although the System Acquisition and Implementation Standard established by IT states that all software should be reviewed by IT, departments often use procurement cards to purchase software with a cost of less than \$3,000. In this case, software purchases may not be reviewed by IT prior to purchase. It also appears that if the purchase is made as a sole source or from the State of Texas Cooperative, and other authorized purchasing cooperatives such, as GSA, TIPS, and Buyboard (use of purchasing cooperatives authorized by the City's Purchasing Department) program for amounts between \$3,000 and \$49,999, or funds are available in departmental budgets, oversight from the IT governance process can be minimal. Purchases of \$50,000 or more require Council approval and, as noted, are generally subject to the IT governance process.

Audit Results

The master list of Citywide hosted applications was obtained from the City's IT department. The accuracy and completeness of the listed applications was validated in meetings with departmental technology staff. The list was then updated accordingly (See Appendix B). A statistically valid sample, based on data value and risk, at a 95% confidence level, was selected. This resulted in a sample size of 30 software solutions. It should be noted some hosted solution acquisitions date back 10 or more years, while other software solutions were purchased relatively recently. The sample was subjected to a review process, as described below:

- Communication with vendors to obtain additional information, such as most recent documents and product related information
- Review of the related SOC2 document, to assess the control environment at the location where Arlington data resides
- Review of Purchasing Card Industry (PCI) compliance if the application processed payments from Arlington citizens
- Review of the vendor contract or service agreement to ensure identified risks to Arlington data are mitigated and efficient operations are supported
- Discussions with user departments' technology staff, as well as IT department management, regarding specific observations and proposed remedial action
- Discussions with the City Attorney's Office on specific contractual and service agreement clauses
- Use of web research and subject matter research from Information Systems Audit and Control Association (ISACA) during audit planning and audit testing phases. ISACA is the leading authority on technology audit and internal controls.

Some of the hosting agreements reviewed include performance clauses specific to the City of Arlington. These are basic vendor commitments stating the software will achieve certain performance standards, such as percentage of availability and work order resolution within a pre-defined time frame. The agreement with the City's accounts payable vendor, Catalyst, includes the greatest number of performance clauses, in addition to software performance. The Catalyst software vendor has committed to invoice processing, payments to vendors, and customer service goals within specific time periods. The Catalyst contract includes a reduction in fees if performance falls below the established thresholds on a continuous basis. As such, the ability to measure results within the software, as well as performance monitoring by City staff, including communications with vendors related to performance, was an important aspect of the audit.



Detailed Audit Findings

A Signed Valid Contract and SOC Compliance is Needed for Team Sideline

Team Sideline, based in California, is a software used by the Parks and Recreation Department. Its use was expanded in February 2020 to include youth sports team registrations, since the software used previously for this purpose was not performing as expected. The following exceptions were noted during audit review:

- A signed, valid contract does not exist, although the vendor had been utilized by the Parks Department for over a decade.
- The vendor stated that their data center in Arizona has not been subjected to a SOC2 assessment or another independent third-party data environment assessment.

Standards and guidelines set forth by the American Institute of Certified Public Accountants (AICPA) require data hosting entities to comply with generally accepted security standards. These standards are intended to protect data and transaction integrity, which is necessary for Arlington Parks operations.

Since the software is used to register youth sports teams for tournaments, data includes personal data, such as names, addresses, contact information of players, parents and coaching staff. The software is used to process payments as well, and the PCI compliance information was submitted by the vendor. The credit card payment processor, Authorize.net, meets data security requirements under PCI guidelines.

As noted, documentation provided by the vendor shows their data center in Arizona has not been subjected to a data security assessment by a qualified third party. The vendor did provide a document; however, it appears to be a self-assessment by the vendor that states their data environment is secure.

The data residing at the vendor hosted site could be susceptible to intrusion, considering there has been no data security assessment by a qualified third party. The City may be held liable in the event of a breach. Also, a reputational risk exists, considering juvenile and adult personal information resides at the vendor site.

Recommendation:

- 1. The City Auditor’s Office recommends the Chief Technology Officer consider working with the Director of Parks and Recreation to obtain a valid contract/service agreement with the Team Sideline vendor that includes necessary security and performance clauses.***

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Enhanced security in the Water Department Twitter account is Needed

The Water Department uses a Twitter social media account to broadcast messages to Arlington residents, regarding matters related to water service and delivery. Some current practices could be considered potential security and operational weaknesses. They are listed below.

- The account is set up as a regular individual social media account using a Yahoo email account.
- User ID's and passwords are shared among three account administrators.
- There is a lack of clear audit trails that would show log-in activity and account use activity.
- Enhanced security practices that are warranted in a business social media account, such as two-point authentication, is not used.

Hosted Applications Audit

The Twitter account is used to inform citizens about water main breaks, service interruptions, and communicate other customer service announcements to Arlington citizens. Messages are broadcast to residents with Twitter accounts and who have signed up to receive notifications. There are two administrators in the Water department and another in the Office of Communication and Legislative Affairs (CLA). Private messages (responses from citizens) are retrieved through the yahoo email account. Citizens can also comment on Twitter notifications that are broadcast to other registered Twitter users.

No fee is associated with the current general use Twitter account using a Yahoo email address. CLA staff noted they use general analytics tools, such as Google and Yahoo, to extract data to measure social media account effectiveness and obtain analytics. It appears that logging into a Google or a Yahoo account is necessary to access the analysis tools. The log-in occurs when signing into the Google or Yahoo email account.

It may be important to note that if the password to the general email account is discovered/compromised, the log-in credentials could be used maliciously to access and broadcast from the Twitter social media account.

Further, the City's current IT policies prohibit sharing of user ID's and passwords. Also, as a good general business practice, City business should be conducted using an official City email address. Content in City email accounts are usually more secure than when using general email accounts, which can be more susceptible to hacking. Also, generally accepted IT software controls recommend use of audit trails to link transactions to the users performing the transactions.

Audit's research on types of Twitter accounts indicated the availability of accounts designated for business entities. These accounts appear to offer better security, content management, audit trails and the measuring of the effectiveness of social media, all included in one package. These business accounts are usually fee based. The information provided by using these types of accounts is highly sought by business users.

Recommendation:

- 4. The City Auditor's Office recommends the Chief Technology Officer consider working with the Director of Water Utilities to explore the use of a business Twitter account for broadcasting social media messages to Arlington citizens and use a City Email account to receive citizen feedback and as log-in credentials to Twitter.***

Hosted Software Performance Monitoring is Needed

The audit included reviewing contract clauses that include vendor commitments for performance levels specific to the City. A reliable and consistent method to assess compliance with the software availability clauses does not exist for all software. Compliance is best measured via tools embedded within the application. Tools outside the application that track performance are dependent on manual processes for data entry and, therefore, are not as reliable and accurate.

Hosted Applications Audit

Thirty hosted agreements were reviewed during the audit. Five contracts containing Arlington-specific performance clauses were selected from the sample of 30. Details about the selected clauses are discussed below.

The following hosted software contracts include performance clauses related to software availability. Generally, the vendor pledged software availability at above 90%.

- **Body Worn Camera Software** - used by the Police department to record officer interaction with citizens
- **Asset Works Software** - used by the City's fleet division to process maintenance and repairs of City owned vehicles
- **Cartegraph Software** - used by the Public Works Department to process work orders and track inventory
- **Brazos Software** - used by the Police Department to issue citations and then upload for the Municipal Court

The following software includes performance clauses promising to process transactions within specific time periods.

- **Catalyst Accounts Payable Software** - used by the Finance Department to process vendor payments

Vendors generally pledge that they can process transactions and deliver software performance exceeding 90% of the time, per the agreement. Often vendors offer rebates when these levels are not met, however the four examples above pledging *availability* did not.

The Catalyst accounts payable software performance clauses include pledges to process invoices, issue payments, keep error rates low, and answer service inquiries within specific time periods. As noted earlier in the report, Catalyst does consider it a breach of contract and offers compensation when expectations are not met, per the contract. To date, Catalyst has not been required to refund or reduce fees due to unmet expectations.

The following affect the availability of hosted software:

- Availability of the hosted website, which is based on the robustness of the vendor's or cloud-site web infrastructure
- Availability of the application itself, its lack of defects, and the ability to use all the software functionality

Hosted Applications Audit

For each of the four hosted application contracts reviewed that include software *availability* clauses, when an issue arises, the departments' system administrators directly submit notices of software malfunctions and errors to the vendor, via a work order submission process. Reports of past work order history can usually be generated for specific periods to review the types and frequencies of issues; however, tools are not available within the software to determine if the malfunction or error resulted in the software being unavailable. Lack of availability is not necessarily linked to malfunctions or errors.

It was noted the Catalyst software, which includes clauses promising to process transactions within specific time periods, *does* have the capability of tracking transaction processing efficiency, including built in reports that can be generated for specific time periods. The reports, however, are not consistently monitored or reviewed by Finance staff.

It appears that vendor pledges included in performance clauses in hosted service agreements are not examined for compliance by the user departments consistently. Additionally, or perhaps as a result, vendors have typically not embedded software measurement tools in hosted applications.

Performance statistics for hosted applications are important in assessing whether the vendor is performing as promised per the agreement. These statistics may be instrumental in deciding to continue using a software or when negotiating with a vendor in future contract matters.

Recommendations:

5. ***The City Auditor's Office recommends the Chief Technology Officer request that IT staff coordinate with the individual departments that utilize the referenced software products and work with the vendors to produce a reliable performance monitoring tool within the software to assess contract compliance.***

6. ***The City Auditor's Office recommends the Chief Technology Officer consider working with the Chief Financial Officer to ensure Finance department staff consistently monitor and retain Catalyst software performance data to determine contract compliance.***

Monitoring Connectivity to Hosted Sites is Needed

The success of a hosted application also depends on robust internet access within the City's own infrastructure. Internet access services are usually provided by vendors such as CenturyLink and Spectrum, commonly referred to as Internet Service Providers (ISP). Solar Winds Net Path is a software product available in the IT department that can monitor the availability of a website (i.e. it can monitor the connectivity between the COA network and the external website). However, currently Solar Winds Net Path is not consistently utilized to monitor the connectivity between the City's network and the hosted websites.

The City's ISP capabilities are crucial, considering it can provide uninterrupted and fast access to hosted web applications. As the City's use of hosted services has increased steadily, providing a

Hosted Applications Audit

reliable path to these applications has now become an important aspect of their use. The availability of hosted services and the need to monitor access to them from our own internal network is critical for many City operations.

The current use of Solar Winds Net Path software is based on need, such as when connectivity needs monitoring during troubleshooting, and is not used to monitor web connectivity on a more global basis. It is important to note that prior to global use of Solar Winds Net Path, some assistance from its vendor, as well as the actual hosted sites the City intends to monitor, may be necessary. Monitoring attempts may set off defensive mechanisms in hosted sites. Also, there may be limitations on how many websites it can monitor at any given time. Coordination with the Solar Winds Net Path vendor, as well as hosted site owners, can mitigate any negative aspects related to the use of the software. As identified earlier, hosted site availability and performance monitoring is best accomplished with tools embedded within the vendor software. However, the use of the Solar Winds Net Path would be helpful to determine if problems exist in our infrastructure that inhibit an uninterrupted path from the City's network to a hosted environment.

If the number of hosted sites that Solar winds Net Path can monitor is limited, monitoring activities could be selected based on critical impact on City operations and volume of users accessing the hosted application. A rotating monitoring schedule is also an option, based on Solar Winds Net Path capabilities.

Solar Winds Net Path can provide detailed information, such as data travel patterns within the city's network to the external sites and to identify bottlenecks. Internet availability data generated from the use of Solar Winds Net Path can be communicated to the City's internet service providers with the intent to improve service.

Recommendation:

- 7. The City Auditor's Office recommends the Chief Technology Officer consider the use of Solar Winds Net Path software to determine the efficiency of Citywide Internet access and its impact on accessing hosted applications and their features.***

[REDACTED]

[REDACTED]

[REDACTED]

Hosted Applications Audit

[Redacted]

[Redacted]

- Build and Maintain a Secure Network and Systems
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy

Level of compliance is also dependent on the amount of transactions, with the top tier being level 1 at over 6 million transactions and lowest level being level 4, below 20,000 transactions a year. The Finance department's Treasury division ranks City of Arlington in-person transactions as a level 3, between 20,000 and 1 million transactions.

[Redacted]

[Redacted]

[Redacted]

[Redacted]

Hosted Applications Audit

Key Internal Controls and Contract Clauses are Needed

Earlier in the report we noted certain performance related pledges included in a few software applications we reviewed. However, we noted a lack of key contract clauses that would result in better internal controls in our review of a sample of 30 hosted application contracts. If included, these controls would provide improved operational controls and help ensure vendors provide beneficial, timely services to the City. These features would also provide legal recourse if vendor services are discontinued or there is a breach associated with the City's data. The following describe some of these key aspects:

- **Software Availability** - A commitment to ensure software is available for use based on days and hours. As noted earlier, vendors usually commit to a 90% or above availability.
- **Incident Response** - A commitment to correct software errors with a time frame based on the level of criticality.
- **Software Updates** - A commitment to update application software on a regular basis, as needed operationally
- **Security Controls** - A commitment to enhance application security based on security threats, vulnerabilities, and operational needs.
- **Compliance Requirements** - A commitment to adhere to security standards based on data categorization, such as HIPAA standards.
- **Exit Strategy** - A commitment to return Arlington data in a usable format in the event of vendor termination, within a specific time period after contract end date.
- **Cyber Security Insurance** - A commitment to indemnify the City against liability arising from cyber security and data breaches. This usually includes a clause to protect high value data, such as public safety records and financial records. Most City data is public information.

Exceptions to the above are noted in the table below (an "X" depicts where an aspect mentioned above is absent or in need of improvement).

Hosted Applications Audit

| | | Software Availability | Incident Response | Software Updates | Security Controls | Compliance Requirements | Exit Strategy | Cyber Insurance |
|---------------|-------------------|-----------------------|-------------------|------------------|-------------------|-------------------------|---------------|-----------------|
| Software Name | Purpose | | | | | | | |
| Ecolane | Handitran | | | | | X | X | |
| E-Builder | Capital Projects | | | | | | X | |
| CCMSI | Workmans Comp. | X | | | X | | | |
| Cornerstone | HR Jobs | X | X | X | X | X | X | X |
| Better Impact | Volunteer Mgmt | | X | | | | X | |
| Blue Beam | Plan Review | X | X | | | | X | |
| Cartegraph | Workorder Mgmt | | | | | | X | |
| Housing Pro | Housing Mgmt | | X | | | | | |
| SI Play | Sports Teams | | | | X | | X | |
| VS Tracking | Victim Svcs | X | X | | | | | X |
| Lumen | APD Data Analysis | | | | | | X | |
| Ion Wave | Purchasing | | | | | | X | |
| AvailWeb | Body Worn Camera | | | | | | | X |

The current IT governance process, in effect since 2013, provides oversight and guidance to City departments on technology implementations. It offers technical knowledge, project planning, assistance with vendors, product selection, and assistance to determine compatibility with the existing technology infrastructure. The process is used mainly for larger implementation projects that exceed a cost threshold of \$50,000 or require more than 80 hours of IT staff resources. The Project Management Office in the IT department provides assistance to the departments. The IT Project Management Office includes business analysts, project managers, and software specialists. Their activities are also coordinated with staff in the City's Purchasing division.

The IT department currently has a document on its portal entitled "System Acquisition & Implementation Standard" that states technology purchases should be reviewed by IT. However, procurement cards are often used for purchases less than \$3,000, including those for software applications. These purchases may not receive benefit of the IT department review and oversight process, to ensure proper controls are present. It is important to note, however, the IT department is in the process of creating new checklists and best practices that they plan to publish and then establish a process for departments to follow when adding new software to help ensure appropriate review of proposed new software.

Some of the exceptions noted in the table above are related to software purchases that are below the \$3,000 threshold and those acquired prior to the establishment of the IT governance process.

Departments often purchase hosted software and enter agreements that do not include needed clauses specific to the City of Arlington. The vendors provide user agreements that are common to all their customers, and it appears that requests for deviations on contract clauses to meet specific client needs may not be welcomed by the vendors. User departments, with or without IT governance oversight,

Hosted Applications Audit

often agree to these contracts because of operational needs rather than desired internal controls. Control aspects, as noted in this report that are needed for data security and operational efficiency, and which benefit the user, may be absent in these standard user agreements. Vendors may require additional payment for these controls; however, important controls, such as returning the City's own data after termination, compliance with laws, and software availability should not incur an additional cost for the vendor.

The following can result from the lack of key controls and specific contract clauses that benefit the software user:

- Inability to hold vendors responsible for necessary system availability and timely error correction, which are needed for effective operations and achieving business objectives
- Lack of timely software updates that can lead to security related exposures resulting in data breaches
- Unauthorized access when controls such as password standards and change policies are not in place
- Liability to the user (City) arising from vendor noncompliance with certain standards, such as HIPAA and juvenile record protection, etc.
- Lack of contractual commitment by the vendor to provide the City with its own data after expiration of the software agreement and/or the City's inability to convert the data to a usable format going forward
- City's liability in the event of a cyber breach and data exposure when vendors are not contractually committed to provide cyber security insurance

Recommendation:

- 9. The City Auditor's Office recommends the Chief Technology Officer identify a methodology to ensure departmental software purchases are reviewed by IT staff to ensure adequate internal control requirements are met, based on risk related to operational or financial data significance, regardless of cost or method of purchase.***

ActiveNet SOC Compliance is Needed

The City's Parks and Recreation department uses ActiveNet hosted software as its enterprise system. When requested by Internal Audit, the vendor failed to produce a valid SOC2 (Service Organization Controls) document to attest to their compliance with generally accepted data security and compliance standards. The vendor initially informed Internal Audit that the data is hosted at an Amazon cloud site. However, when later asked for the appropriate documentation, the vendor stated the data is stored in a self-owned data center in Las Vegas, Nevada and their compliance status is unknown. The

Hosted Applications Audit

request to provide the necessary documentation was communicated to the vendor in January 2020, and we had not received a response as of the end of audit fieldwork.

The sensitive data contained in the system includes names, dates of birth, phone numbers, addresses, email addresses and credit card information. The vendor is PCI compliant in its processing of card payments. ActiveNet is used to process the following transactions daily:

- Front desk administration of customer accounts and payments
- Online user account creation and management
- Online registration for activities
- Online memberships
- Use of coupons during online processing
- Scheduling of all recreation, athletic and rental facilities
- Flex (flexible options) Reg (registration) for day camps (single day registrants or week-long participation)
- Reporting
- Financial management of accounts
- Custom financial export transferable to Lawson

As noted earlier in this report, the SOC2 review process has been designated as an acceptable control assessment for hosted data centers. The standard was created by the American Institute of Certified Public Accountants and outlines various security practices, including data storage standards, data backup and recovery, updates to software, risk mitigation and cyber security, as well as other standards. Assessment and compliance should be reviewed annually by a non-affiliated third party. The intention of the standard is to help protect data and transaction integrity.

The ActiveNet software was implemented with assistance from the IT governance team in 2015. The project management team reviewed compliance documents, such as SOC reports and PCI compliance reports, at the time of system implementation. However, the data centers and credit card processing servicing for ActiveNet has changed since implementation. The reason for current noncompliance is unknown.

Transaction integrity and security in hosted solutions are dependent on the compliance and control environment at the data center. Considering the sensitive nature of the data at ActiveNet, it is necessary to obtain an assurance the vendor is following accepted protocol at the data center. In the absence of such assurance, data breaches could occur and result in a liability to the City and could present a reputational risk.

Recommendation:

- 10. The City Auditor's Office recommends the Chief Technology Officer consider working with the Director of Parks and Recreation to request that the ActiveNet vendor comply with generally accepted control standards and provide a SOC2 assessment report. The assessment should be completed by a qualified third-party assessor within a designated***

Hosted Applications Audit

timeframe. If the vendor fails to comply timely, the Chief Technology Officer, in collaboration with the Director of Parks and Recreation, should seek assistance from the City Attorney's Office to determine if the software contract has been breached and what further action should be taken.






AUDIT RECOMMENDATIONS AND MANAGEMENT RESPONSE

| RECOMMENDATION | CONCUR/ DO NOT CONCUR | MANAGEMENT RESPONSE | RESPONSIBLE PARTY | DUE DATE |
|--|-----------------------------|---|----------------------|-------------------|
| <p>1. <i>The City Auditor's Office recommends the Chief Technology Officer consider working with the Director of Parks and Recreation to obtain a valid contract/service agreement with the Team Sideline vendor that includes necessary security and performance clauses.</i></p> | <p>CONCUR</p> | <p>The IT Department will work with the Parks and Recreation Department to obtain a valid contract/service agreement with the Team Sideline vendor that includes the necessary security and performance clauses. The Team Sideline website provides a privacy policy that does not provide security controls information.</p> | <p>IT and PARD</p> | <p>08/01/2021</p> |
| <p>[REDACTED]</p> | <p>[REDACTED]</p> | <p>[REDACTED]</p> | <p>[REDACTED]</p> | <p>[REDACTED]</p> |
| <p>[REDACTED]</p> | <p>[REDACTED]</p> | <p>[REDACTED]</p> | <p>[REDACTED]</p> | <p>[REDACTED]</p> |

Hosted Applications Audit

| | | | | |
|---|---------------|---|-------------------------------|-------------------|
| | | | | |
| <p>4. <i>The City Auditor's Office recommends the Chief Technology Officer consider working with the Director of Water Utilities to explore the use of a business Twitter account for broadcasting social media messages to Arlington citizens and use a City Email account to receive citizen feedback and as log-in credentials to Twitter.</i></p> | <p>CONCUR</p> | <p>The IT Department will work with Water Utilities and update the current Twitter account. The account will be aligned with the existing Social Media Usage, Standard Operating Procedure updated in 2018 by Communication and Legislative Affairs.</p> | <p>IT and Water Utilities</p> | <p>12/01/2020</p> |
| <p>5. <i>The City Auditor's Office recommends the Chief Technology Officer request that IT staff coordinate with the individual departments that utilize the referenced software products and work with the vendors to produce a reliable performance monitoring tool within the software to assess contract compliance.</i></p> | <p>CONCUR</p> | <p>The IT Department will work with our Departments to review our software contracts for performance monitoring clauses. If the current contract lacks performance controls, our IT Department will provide guidance for such performance measures during the contract renewal process.</p> | <p>All City Departments</p> | <p>10/01/2022</p> |
| <p>6. <i>The City Auditor's Office recommends the Chief Technology Officer consider working with the Chief Financial Officer to ensure Finance department staff consistently monitor and retain Catalyst software performance data to determine contract compliance.</i></p> | <p>CONCUR</p> | <p>The AP Supervisor and Controller receive weekly performance data reports from Catalyst that are monitored and retained for contract compliance purposes. Finance staff will document review. Finance reviewed this calendar year's reports and noted no non-compliance.</p> | <p>Finance</p> | <p>10/31/2020</p> |
| <p>7. <i>The City Auditor's Office recommends the Chief Technology Officer consider the use of Solar Winds Net Path software to determine the efficiency of Citywide Internet access and its impact on</i></p> | <p>CONCUR</p> | <p>The IT Department will work with SolarWinds to properly implement NetPath monitoring for hosted solutions. As noted in the audit response, if NetPath has limitations to the number of sites</p> | <p>Information Technology</p> | <p>03/01/2021</p> |

Hosted Applications Audit

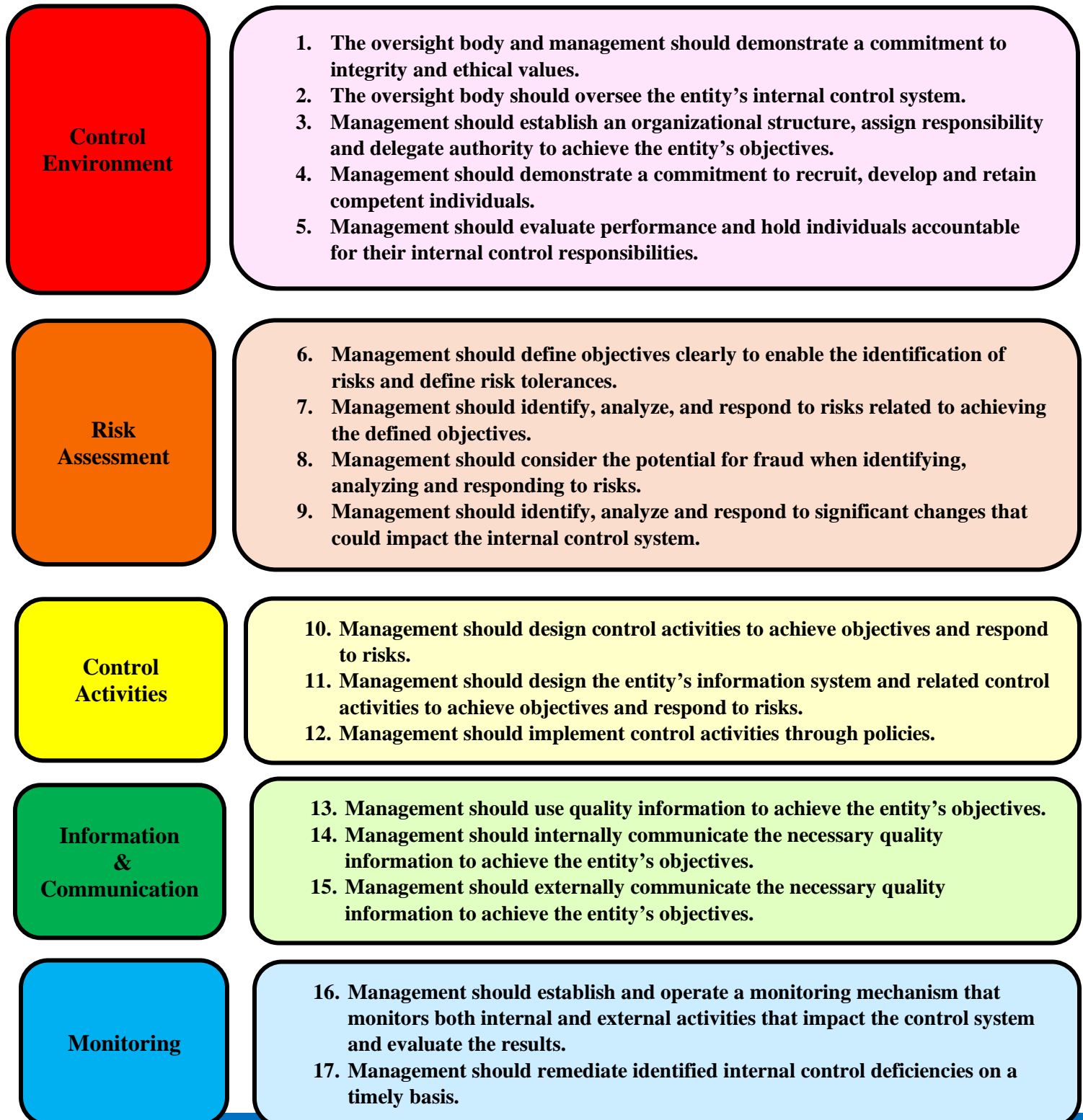
| | | | | |
|---|---|--|---|---|
| <p><i>accessing hosted applications and their features.</i></p> | | <p>monitored, we will focus on those systems with the highest impact to the organization.</p> | | |
|  |  |  |  |  |
| <p>9. The City Auditor’s Office recommends the Chief Technology Officer identify a methodology to ensure departmental software purchases are reviewed by IT staff to ensure adequate internal control requirements are met, based on risk related to operational or financial data significance, regardless of cost or method of purchase.</p> | <p>CONCUR</p> | <p>The IT Department will coordinate with Purchasing to refine our existing procurement process, Technology Purchase Request (TPR). Our recommended TPR will provide our departments guidance on, TPR Submittal Process, Funding Requirements, IT Department Approvals. The TPR process will provide improved controls that will include risk management and vendor management. Additional recommendations will include discontinuing the use of the P-Card for technology purchases with some exceptions, such as peripheral devices.</p> | <p>Information Technology and Purchasing</p> | <p>05/01/2021</p> |

Hosted Applications Audit

| | | | | |
|--|--------|---|---|------------|
| <p><i>10. The City Auditor's Office recommends the Chief Technology Officer consider working with the Director of Parks and Recreation to request that the ActiveNet vendor comply with generally accepted control standards and provide a SOC2 assessment report. The assessment should be completed by a qualified third-party assessor within a designated timeframe. If the vendor fails to comply timely, the Chief Information Officer, in collaboration with the Director of Parks and Recreation, should seek assistance from the City Attorney's Office to determine if the software contract has been breached and what further action should be taken.</i></p> | CONCUR | <p>The IT Department will work with the Parks and Recreation Department to request that the ActiveNet vendor comply with generally accepted control standards and provide a SOC2 assessment report. During the initial contract award, ActiveNet was determined to be SOC2 compliant and the vendor produced assessment documentation demonstrating their compliance. A follow-up compliance review will be coordinated with the vendor. If the vendor fails to comply with the agreed upon contractual requirements, the Chief Technology Officer, in collaboration with the Director of Parks and Recreation, will seek assistance from the City Attorney's Office to determine if the software contract has been breached and what further action should be taken.</p> | Parks and Recreation Department and Information Technology Department | 08/01/2021 |
|--|--------|---|---|------------|

Appendix A

The Five Components and 17 Principles of Internal Control



Appendix B – Hosted Applications

| Name of Software | Purpose | User Department |
|-------------------------|------------------------------|------------------------|
| CitiBot | Citizen engagement tool | Action Center |
| Accela | Citizen complaints | Action Center |
| GovMax | Departmental budgets | Finance |
| State of TX – Ethics | Form 1295 filings | Finance |
| Teammate | Electronic Audit Workpapers | Internal Audit |
| LexisNexis | Attorney search tool | City Attorney's Ofc |
| CivicLive | Website content management | Mgmt. Services |
| InspectCheck | Multifamily inspections | Code Compliance |
| Petango | Pet search services | Animal Services |
| Insite | Credit card processing | Municipal Court |
| GovQa | Open record requests | City Attorney's Ofc |
| Granicus | Council Meetings | City Secretary Ofc |
| American Express | Credit card management | Finance |
| Arlington Webstore | Webstore sales and records | Finance |
| Authorize.net | Credit card management | Finance |
| Bank of America | Health care claims backup | Finance |
| Braintree | Credit Card management | Finance |
| Echo | Grant reimbursement requests | Finance |
| Elavon | Credit card management | Finance |
| Federal tax systems | Payroll taxes | Finance |
| Employer E Services | Healthcare claims reports | Finance |
| Global Payments | Credit card management | HR |
| Grant Thornton | External Audit schedules | Finance |
| Grants.gov | Search for grants | Finance |
| US Dept of Treasury | Grant reporting | Finance |
| Merchant Connect | Credit card management | Finance |
| Open Edge | Credit card management | Finance |
| Payment Tech | Credit card management | Finance |
| Award Management | Grant registration | Finance |
| Tarrant County | Property tax payments | Finance |
| Texnet | Court fees and fines | Finance |
| TMRS City Portal | Employee retirement | Finance |
| TrAMS | Grant reporting | Finance |
| TXDOT | Grant reporting | Finance |
| Vanguard | Monthly investment data | Finance |
| Access | Chase banking | Finance |
| CIMRS | Managing CALEA reports | Fire |
| CrewSense | Scheduling software | Fire |

| Name of Software | Purpose | User Department |
|---------------------------|------------------------------------|------------------------|
| ECaTS | 911 reporting application | Fire |
| Everbridge | Citizen and staff notifications | Fire |
| Firehouse | Fire enterprise system | Fire |
| Guardian | Early warning, staff recognition | Fire |
| Power DMS | CALEA accreditation records | Fire |
| Target Solutions | Public safety training | Fire |
| Network Fleet | City vehicle management | Fleet Services |
| ESRI | GIS software | IT |
| Ecolane | Passenger scheduling | Handitran |
| AVAYA | Phone management | Housing |
| Housing Pro | Enterprise housing management | Housing |
| HUD system | Housing program management | Housing |
| State contract system | Housing statistical information | Housing |
| Allstate | Accident Illness plans | HR |
| Better Impact | Volunteer management | HR |
| CareATC | Employee clinic | HR |
| Cornerstone | Staff recruiting system | HR |
| Delta Dental | Staff dental Insurance | HR |
| ETC | Medical plan reporting | HR |
| E-verify | Employment eligibility | HR |
| Hire right | Employee background checks | HR |
| Ice_CCMSI | Workman's comp claims | HR |
| Legal Shield | Employee legal plans | HR |
| Navitus | Pharmacy management | HR |
| Poll everywhere | Training survey platform | HR |
| Prudential | Employee life insurance | HR |
| Superior Vision | Employee vision insurance | HR |
| TX-DPS | Background checks | HR |
| UHC | Employee health insurance | HR |
| Wells Fargo | Benefit plan information, payments | HR |
| Daktronics | Electronic signage system | IT |
| E-Builder | Capital project management | IT |
| Ghin Handicap | Golf Management | IT/Parks |
| Innotas | Project management software | IT |
| Microsoft Office Products | Enterprise software | IT |
| Remedy force | Work order management | IT |
| SDOL – JPM | Credit card management | Finance/IT |
| Stealth monitoring | Golf course monitoring | IT |
| Survey Monkey | Survey management | IT |
| APPSpace | Court video monitoring | IT/Court |
| Visage Club Car | Golf cart management | IT/Parks |
| Lawson | Citywide enterprise management | IT/Finance |
| ICMA-RC | Employee 401k | IT/HR |

| Name of Software | Purpose | User Department |
|-------------------------|----------------------------------|-------------------------|
| Optum bank | Health plan management | IT/HR |
| Wells Fargo | Disability plan payments | IT/HR |
| Active Campaign | Newsletter software | Parks |
| Active Net | Enterprise software | Parks |
| Cartegraph | Asset and work order management | Parks/PW/Water |
| In Tennis | Tennis court management | Parks |
| Issuu | Magazine content management | Parks |
| Litmus | Newsletter test software | Parks |
| SI play | Youth sports management | Parks |
| SkyLogix | Facility lighting management | Parks |
| Wrike | Project and time management | Parks |
| CISCO | HSA payment management | Finance |
| Dept. of Labor | Labor statistics management | Finance/HR |
| Expert Pay | Child support payment management | Finance |
| Social Security Agency | W2 reporting | Finance |
| TX – AG | Child support payment reporting | Finance |
| Constant contact | Direct marketing | Planning & Dev |
| Prominent Modi-Mille | Chemical Management | Parks |
| Perry Weather | Lightning Detection | Parks |
| Thorguard | Lightning detection equipment | Parks |
| Sports Standing | League scheduling | Parks |
| Team Sideline | League scheduling | Parks |
| Fuel Master | Fuel management | Parks |
| 121 Marketing | Golf website content management | Parks |
| Flickr | Online photo management | Parks |
| Google | Advertising, website analytics | Parks |
| Neptune Radio | Personalized radio station | Parks |
| Sprout | Social media dashboard | Parks |
| We Transfer | File sharing site | Parks |
| Quantum | Change order management | Parks |
| EPR | Electronic plan review | Planning & Dev |
| Facebook | Social Media | Multiple Departments |
| Gameday Software | Event management software | Police |
| LexisNexis | Citizen police reports | Police |
| Live Engage | Officer communications | Police |
| Twitter | Social Media | Multiple Departments |
| VS Tracking | Victim management software | Police |
| Crash | Accident reporting | Police |
| Lumen | Search tool | Police |
| Police Mobile | Communication software | Police |
| PowerDMS | Policy and training | Police |
| Brazos | Citation management | Police |

| Name of Software | Purpose | User Department |
|-------------------------|---------------------------------------|------------------------|
| Demand Star | Bid platform | Purchasing |
| IonWave | Electronic bidding notifications | Purchasing |
| Bluebeam | Plan review software | Public Works |
| Field ID | Location sampling | Public Works |
| Connected Signals | Vehicle and infrastructure management | PW |
| Icone Traffic | Traffic control management | PW |
| Trafficware Blue Toad | Bluetooth travel management | PW |
| Access | Banking application | Finance |
| Bloomberg | Investment research | Finance |
| Bond Link | Investment reports | Finance |
| Payment tech Chase | Credit transaction reporting | Finance |
| Diver | Financial disclosures | Finance |
| EMMA | CAFR reporting, debt disclosures | Finance |
| Ipreo | Competitive debt sales | Finance |
| MAC | Debt reporting | Finance |
| Merchant Connect | Transaction reporting | Finance |
| Nexen | Escrow account reporting | Finance |
| PCI Manager | Credit card compliance | Finance |
| State Street | Investment management | Finance |
| Tarrant Appraisal | Property values | Finance |
| Texas Class | Investment purchases | Finance |
| Tex Pool | Investment management | Finance |
| TexStar | Investment management | Finance |
| TexTerm | Investment management | Finance |
| TX Comptroller | Tax and grants reporting | Finance |
| Catalyst | Accounts Payable | Finance |
| Hootsuite | Social media updates | Water |
| Invoice Cloud | Payment processing | Water |
| NextDoor | Social Media | Water |
| Selectron | Voice response system | Water |
| Insta360 | Marketing software | Parks |
| Rainbird | Golf Irrigation | Parks |
| Toro | Golf Irrigation | Parks |
| AvailWeb | Body worn camera | Police |