CITY OF SAN ANTONIO

OFFICE OF THE CITY AUDITOR

Audit of Development Services Department

Accela System Release 2

Project No. AU21-011

April 21, 2022

Kevin W. Barthold, CPA, CIA, CISA
City Auditor

Executive Summary

As part of our annual Audit Plan approved by City Council, we conducted an audit of the Development Services Department (DSD), specifically the Accela System Release 2. The audit objectives, conclusions, and recommendations follow:

Determine if application controls for the Accela system are adequate and data is accurate and reliable.

The Accela system is working as intended by providing a more efficient and effective way for citizens to access City services and pay for those services in a secure manner. We determined that DSD has established policies and procedures to manage password requirements, data entry, change management, interface processing, and server security.

However, there are significant opportunities to strengthen the controls associated with user access, segregation of duties, and revenue account reconciliations, which are the same deficiencies identified in the prior Accela audit (Release 1) completed in 2020. The action plans provided by management were not fully implemented to strengthen controls and mitigate risk. In addition, server backups are not being validated, service-related incidents are not meeting the Service Level Agreement, and open jobs valued at $6,360,238.22 exist that management is unable to determine the current status.

Significant resources may be necessary to address critical issues in a timely manner.

We provided recommendations for each finding for Management to consider resolving the issues identified.

DSD Management agreed with the audit recommendations and have developed positive action plans to address them. Management's verbatim response is in Appendix B on page 9.

Table of Contents

Background

The Development Services Department (DSD) is responsible for coordinating land and building development throughout the City. In partnership with other City departments, DSD helps homeowners, business owners, and those in the commercial industry plan and execute development projects.

For years, DSD has utilized disparate systems to deliver permit, inspection, land development and code enforcement services to their customers. These systems became outdated and were unable to easily adapt to DSD's changing business needs. In 2012, a business need to replace the outdated systems was identified and BuildSA formally initiated. BuildSA is the designated name of the project or software system that has either replaced or integrated with many of the systems used today by DSD. The provider or vendor of the system is Accela.

BuildSA is a web-based solution with workflow capabilities that allow DSD and partnering agencies to review, markup and comment on documents, eliminating the need for paperwork that typically accompanies paper-based reviews. Customers seeking to build, develop or improve property in the City now have access to new capabilities and ways of submitting applications, pulling building and fire permits, making payments and interacting with City and partnering agency staff.

Due to the complexity of DSD business and the amount of resources required to deploy a system like this, the project was divided into two phases that follow the development process:

- Release 1 included activities associated with horizontal development such as zoning, platting and construction inspections (Land Development). Release 1 was implemented on October 1, 2018.
- Release 2 is for activities associated with horizontal construction, such as plan review, permitting, inspections, building-related fire permits and includes code enforcement activities (Building Development & Code Enforcement). Release 2 was implemented on November 30, 2020.

Activities for these releases includes application submission, staff review and approval, invoicing, and payment receipts.

Audit Scope and Methodology

The audit scope was from November 30, 2020 through August 2021.

To establish our test criteria, we reviewed DSD and Information Technology Services Department (ITSD) policies and procedures, system documentation, and user access listings. We interviewed DSD and ITSD management and staff to gain an understanding of the Accela system Release 2 and the supporting infrastructure. Additionally, we reviewed the financial data generated from Accela.

As part of our testing procedures, we examined the following areas.

- User Access
- Password Settings
- Incident Management
- Change Management
- Backup and Recovery
- Interface Processing
- Input/Edit Data Entry
- Performance Measures
- Revenue Collection and Reconciliations
- Refund Processing

We relied on computer-processed data in SAP, the City's accounting system, to verify Accela refund payments were accurate. Our reliance was based on performing direct tests on the data rather than evaluating the system's general and application controls. We do not believe that the absence of testing general and application controls had an effect on the results of our audit.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Audit Results and Recommendations

A. User Access Controls *(repeat finding)*

Controls over privileged and general user access to the Accela system including how users are added and removed are not consistently applied. Specifically, we identified an excessive number of users with privileged (system administrator) access, user access granted without proper authorization, and user access reviews not being performed.

Currently, of 632 Accela active user accounts, 28 accounts have system administrator access which allows them to make major changes to a system and bypass certain security constraints. Additionally, three of the 28 administrator accounts are withdrawn employees, seven accounts have not logged on in over 180 days, and one vendor test account needs to be disabled since the vendor no longer supports Accela.

We identified 11 user accounts assigned to withdrawn employees, three user accounts that were not deactivated timely, and 20 user accounts that have had no activity for over 180 days.

We were unable to verify that new user access requests were approved since majority of new users for Release 2 were added in bulk via a script by the vendor, which is against ITSD's policies.

Finally, we reviewed users who had permissions to process a refund in Accela. We identified 231 employees with the 'DSD Lead' role who have permissions to process a refund within Accela's workflow. Out of the 231 employees, only eight are Finance Administrators that should have permissions to process a refund.

Administrative Directive (AD) 7-8D Access Control states that access permissions will use the principle of least privilege. Additionally, access to City of San Antonio (COSA) IT assets must be disabled upon separation of the employee. Finally, all COSA Information Systems must be periodically screened for inactive accounts.

During the initial implementation of the Accela system, a Security Plan was created and adopted to ensure security elements and vulnerabilities are evaluated. The Security Plan requires that in order to gain access to the Accela production system, all users must complete, sign and obtain the department approvals on the Accela Production User Access Request Form. Furthermore, there is not a requirement or process to conduct user access reviews on a periodic basis. We also determined the Security Plan does not have the CISO's signature and needs to be updated to reflect minor changes since the initial implementation.

User access controls are designed to restrict and detect inappropriate access to computer systems. Effective access controls protect the City's systems from unauthorized access, modification of data, and inappropriate disclosure of information.

A lack of controls for user access increases the risk of unauthorized users, inappropriate access and/or unauthorized modification of data.

Recommendation

The Director of DSD, working with ITSD, should strengthen user access controls for the Accela system by:

1. Restricting privileged access to authorized and appropriate individuals.
2. Performing periodic reviews of access to ensure that all (privileged and general) user access is appropriate.
3. Enforcing the documented process for handling new user access.
4. Ensuring only fiscal staff have permissions to process refunds.
5. Ensuring the Security Plan is current and approved with required signatures.

B. Segregation of Duties *(repeat finding)*

Accela change management duties are not properly segregated. The developers for the Accela system have inappropriate access to edit data in the production environment. Also, we identified the release team has access to the developer's code repository.

A fundamental element of internal control is the segregation of certain key duties. Key duties in change management include developing or modifying the system code in the development environment, reviewing and approving the modification, testing and quality assurance, and deploying the modified code to the production environment.

Segregation of duties is the process of segregating work responsibilities to help ensure critical stages of a process is not under the control of a single individual. The City's Administrative Directive 7.8D-Access Control requires, where technically feasible and appropriate, that segregation of duties be enforced with access controls.

When an inadequate segregation of duties exists, an employee has the ability to conceal errors and/or conduct fraudulent activities.

Recommendation

The Chief Information Officer should ensure appropriate segregation of duties exist between the Accela development and production environments. If segregation of duties is not feasible, a user violation compensating control should be identified and documented.

C. Revenue Account Reconciliations *(repeat finding)*

DSD Fiscal does not have a process to reconcile revenue reported in the Accela system to the City's financial reporting system, SAP.

The source system, Accela, should represent the subledger that supports the transactions posted to the ledger in SAP. Data within SAP is entered via a batch process from Accela and does not maintain transaction level data. Reconciliations are not being performed between Accela and SAP to ensure SAP balances are accurate and supported.

The purpose of a financial reconciliation is to monitor that the transactions from the source system are completely, timely and accurately represented in the ledger.

The lack of a reconciliation was originally discovered during the Accela audit of Release 1 during 2019. Management's action plan was to develop a monthly reconciliation report to summarize the revenue amounts in Accela, ActiveNet, and SAP. During our current audit of Release 2, we determined the Accela Reconciliation Project is still a work in progress with an estimated completion date of February 2022.

Administrative Directive 8.4 Financial Management of Accounts Receivable states that all individual customer accounts and subsidiary records shall be reviewed and reconciled on a monthly basis to the financial records of the City. This reconciliation process shall be reviewed and signed off by a supervisor.

Without appropriate and routine reconciliations, the City risks misappropriation of revenue and incorrect general ledger allocations.

Recommendation

The Director of DSD, working with ITSD, should continue efforts to ensure a reconciliation of revenue is occurring between Accela and SAP on a monthly basis. Additionally, the reconciliation should be reviewed and approved by appropriate supervisor.

D. Backup and Recovery

The data backups for the Accela servers are not periodically tested to verify their integrity and their ability to be restored. Additionally, procedures do not exist for the restore process.

ITSD relies on the backup tool's alert messages to notify them of any failures that may occur with the automated backups. We did verify that the backup tools send alerts to ITSD's backup and storage team for failures that occur.

The National Institute of Standards and Technology (NIST) Special Publication 800-209 Security Guidelines for Storage Infrastructure say to periodically test backups (at least monthly for critical data) to verify their integrity and their ability to be restored.

Lack of controls to validate system backups could result in a loss of data in the event a backup is corrupted or fails.

Recommendation

The Chief Information Officer should establish a process to periodically test backups and the ability to perform a full restore for the Accela servers.

E. Incident Management

Service-related incidents for the Accela system do not meet resolution times specified in the Service Level Agreement (SLA).

We identified 54 out of 83 (65%) incident tickets did not meet the SLA resolution times. Unresolved incidents are continuously monitored and discussed three times weekly between ITSD Application Support and DSD Support teams, with critical and high priority as their focus.

The SLA between Development Services Department (DSD) and ITSD specifies response and resolution times to provide consistent IT service support and delivery to DSD customers by ITSD.

Untimely resolution times for service-related incidents could lead to application downtime for critical business transactions, and disgruntled customers.

Recommendation

The Director of DSD, working with ITSD, should ensure response and resolution times for service-related incidents comply with the SLA resolution times.

F. Open Jobs

As of August 26, 2021, Accela reported open jobs valued at $6,360,238.22. These open jobs are an indicator of work and revenue that could be earned by DSD if the customer proceeds with the application review and permit process. Several of these open jobs are outside the eligible date of work and may no longer be viable. However, DSD was unable to determine the status of these open jobs and what may still be eligible for reviews and permitting if the customer proceeds with the application. There are some projects/applications in Accela that should be canceled, and fees voided due to customers not moving forward with the application within the required time period. Of the total open jobs within Accela, $1,800,349 are for transactions greater than 180 days old. If the customer has taken no action on submitted applications, they expire at 180 days and any open jobs along with their potential revenue should be removed.

Without a process to monitor and verify the open jobs, DSD does not have accurate information regarding its potential revenue and upcoming workload. Information within Accela should be accurate and reliable for management's decision-making processes.

Recommendation

The Director of DSD, working with Finance, should develop and document a process to determine which open jobs have true and current receivables owed against them for collection, which are open and available for future potential revenue, and which need to be closed out and removed from the potential revenue earnings (pending fees) report.

Appendix A – Staff Acknowledgement

Gabe Trevino, CISA, Audit Manager
Holly Williams, CISA, CRISC, Auditor in Charge
Loretta Faxlanger, Auditor

Appendix B – Management Response

CITY OF SAN ANTONIO
SAN ANTONIO TEXAS 78283-3966

March 18, 2022

Kevin W. Barthold, CPA, CIA, CISA
City Auditor
San Antonio, Texas

RE: Management's Corrective Action Plan for Accela System Release 2

Development Services Department has reviewed the audit report and has developed the Corrective Action Plans below corresponding to report recommendations.

Recommendation					
#	Description	Audit Report Page	Accept, Decline	Responsible Person's Name/Title	Completion Date
1	**User Access Controls** The Director of DSD, working with ITSD, should strengthen user access controls for the Accela system by: 1. Restricting privileged access to authorized and appropriate individuals. 2. Performing periodic reviews of access to ensure that all (privileged and general) user access is appropriate. 3. Enforcing the documented process for handling new user access. 4. Ensuring only fiscal staff have permissions to process refunds. 5. Ensuring the Security Plan is current and approved with required signatures.	4	Accept	(DSD) Patricia Cavazos (ITSD) Michael Fierros	Complete; Resumed October 2021 and reoccurs quarterly #5 May 2022

Recommendation					
#	Description	Audit Report Page	Accept, Decline	Responsible Person's Name/Title	Completion Date
	Action plan: **1. Restricting privileged access to authorized and appropriate individuals.** DSD and ITSD have standardized this process to fix gaps identified. Individuals requesting access to the Accela Civic platform are required to complete an Accela Access Request Form, located on the COSA Forms Net. The document requires that users provide information related to the type of request (new user, modify existing user, and deactivate user) and the role for which access is being requested. The document also supports a multi-user list of individuals requesting the same type and level of access. Forms are submitted to DSD, reviewed, and require signatures from the Department APS/Designee. Forms are then submitted to ITSD by submitting a Service Ticket via the Remedy portal. ITSD completes the provisioning of the user account. **2. Performing periodic reviews of access to ensure that all (privileged and general) user access is appropriate.** A process for performing periodic reviews of access was developed and implemented during 2020. Periodic review meetings started in October 2021 and are scheduled to occur on a quarterly basis. The last quarterly meeting occurred December 13, 2021. **3. Enforcing the documented process for handling new user access.** See Management Response to #1 above. DSD Department APS/Designee is responsible for reviewing and approving all new user access. **4. Ensuring only fiscal staff have permissions to process refunds.** The ability to create a "Finance Administrator Role" (more granular than the current DSD role) with permissions to process a refund, needs to be built into the system. Work order has been created and has been assigned to the next development sprint, anticipated complete in second quarter of FY 2022. **5. Ensuring the Security Plan is current and approved with required signatures.** The System Security Plan has been re-submitted to the Security Team for review and updating and will be signed off by end of April, 2022. Subsequent reviews will be scheduled to occur annually as part of the product management plan for the Accela Civic platform.				
2	**Segregation of Duties** The Chief Information Officer should ensure appropriate segregation of duties exist between the Accela development and production environments. If segregation of duties is not feasible, a user violation compensating control should be identified and documented.	5	Accept	(ITSD) Jeannette Kriewald, Michael Fierros	April 2022

Recommendation					
#	Description	Audit Report Page	Accept, Decline	Responsible Person's Name/Title	Completion Date
	Action plan: There are currently 5 ITSD positions allocated to provide support and development for the Accela Civic Platform. 1 vacant position and 1 team member are assigned to product development, 2 members assigned strictly to support, and 1 member dedicated to report development. Our original action plan in response to the Release I audit was to reconstruct the team to prevent developers from implementing their own developed code. However, it was later determined that this re-organization will negatively impact the team's velocity for development and support because the number of developers would be decreased by 1 person. The updated Action Plan below is recommended to overcome this finding: 1. Developed code will follow a process that includes check points and reviews before it is presented for a production code migration. 2. A team Lead will be designated as the Release Manager. This role will become responsible for the review and approval of the list of tickets and programs scheduled for a production release. 3. Migration of code between environments (Development to Staging or Prod Support to Prod Support Test) will be performed by a developer other than the person who developed the code. 4. Prior to code migrating from Staging or Prod Support Test to Production, it will undergo a peer review and approval. 5. Prior to a production code migration, the Release manager will review and approve tickets for all code modifications scheduled for release from the Staging or Prod Support Test environments.				
3	**Revenue Account Reconciliations** The Director of DSD, working with ITSD, should continue efforts to ensure a reconciliation of revenue is occurring between Accela and SAP on a monthly basis. Additionally, the reconciliation should be reviewed and approved by appropriate supervisor.	5	Accept	(Finance) Melanie S. Keeton (DSD) Veronica Castro (ITSD) Liliana Martinez	July 2022

Recommendation					
#	Description	Audit Report Page	Accept, Decline	Responsible Person's Name/Title	Completion Date
	Action plan: DSD will continue to use existing tools, including the variance dashboards created by ITSD, to (a) identify discrepancies between the Accela and Activenet systems for specific sets of records and (b) cleanse the data associated with these records in the Accela system on a weekly basis and/or as discrepancies are identified or (c) make adjustments to customers' accounts when multiple payments have posted, or have not posted, in Activenet. This effort, which currently includes the equivalent of 2.2 FTEs from DSD and 0.9 FTE from ITSD, allows staff to cleanse the data within Accela and Activenet for comparison across the two systems while also decreasing the variance to $0.00 as much as possible. Final sign-off from Finance will occur on a monthly basis. In addition, DSD and ITSD will update the monthly reconciliation report which will help summarize the revenue amounts in Accela, Activenet (Point of Sale), and SAP. Several iterations of the report have already been completed since the first audit of Accela Release 1 in 2020 and the teams continue to work together to complete the necessary research needed to compare revenue across the three systems. DSD, ITSD and Finance will hold a scoping meeting to determine if it is feasible to accomplish reconciliation across the three systems so that a more automated process can be developed. The current process is manual.				
4	**Backup and Recovery** The Chief Information Officer should establish a process to periodically test backups and the ability to perform a full restore for the Accela servers.	6	Accept	(ITSD) John Rodriguez	Complete

Recommendation					
#	Description	Audit Report Page	Accept, Decline	Responsible Person's Name/Title	Completion Date
	Action plan: An updated restore procedure for moving a copy of the Acella database into production will be complete by March 25, 2022. ITSD believes it is compliant with NIST 800-29 Security Guidelines for Storage Infrastructure for critical data in the Acella environment. All critical Acella data is stored in the SQL Database. The Accela database is currently 920 GB in size and a copy is restored from backup every morning at 2AM and completes by 4AM. This database copy serves as a read-only copy for Acella reporting purposes. ITSD also routinely restores the database transactional logs from the primary backup as well so that a complete database restore (last full backup + transaction log backups) can be used for the reporting server and is used by all customers daily. ITSD does not have the personnel or computing resources to test all Accella production server backups on a routine basis, however, ITSD does perform two functions which provides high confidence in our backups and ability to restore: 1. ITSD routinely restores specific files from Acella production backups with no issue. 2. ITSD routinely restores and validates multiple files or entire systems for different production and non-production systems and databases and has never encountered an issue with corruption in a backup or any problems successfully restoring files. ITSD has high confidence in our backup platform which performs integrity validations of the backup package and is then locked to prevent any changes. Backups are "Forever full", meaning that we can recover a file or system from any backup with a single restore job. Once completed, backups are automatically replicated between datacenters. Backups are also "immutable" which means they are protected from ransomware attacks or changes once saved to the Rubrik system.				
5	**Backlog of Incident Tickets** The Director of DSD, working with ITSD, should ensure response and resolution times for service-related incidents comply with the SLA resolution times.	**7**	Accept	(DSD) Patricia Cavazos (ITSD) Michael Fierros	March 2022
	Action plan DSD and ITSD will review the number of incidents on a monthly basis. ITSD will negotiate prioritization with DSD when the SLA is not met or at risk of not meeting the SLA.				

Recommendation					
#	Description	Audit Report Page	Accept, Decline	Responsible Person's Name/Title	Completion Date
6	**Open Jobs** The Director of DSD, working with Finance, should develop and document a process to determine which open jobs have true and current receivables owed against them for collection, which are open and available for future potential revenue, and which need to be closed out and removed from the potential revenue earnings (pending fees) report.	7	Accept	(DSD) Patricia Cavazos (Finance) Melanie S. Keeton	Complete
	Action plan: DSD staff, in collaboration with Finance, will review the open jobs (pending fee) report to 1) close jobs that are beyond the 180-day active application period; and 2) remove jobs that were inaccurately duplicated as part of the system conversion. Related to item 1, the City's building code states that a project expires if the permit application is not acted upon by the applicant within 180 days of initial submission or if there is 6-months of inactivity on the project. There are times when an applicant chooses not to pursue their project and the project application expires. When this is the case, DSDs monthly review of these expired application will remove these fees from Accela as they are in fact not due if the project never began and no services were rendered. DSD will additionally reach out to customers for outstanding balances on any projects that did have services rendered and therefore fees owed for work that has been performed on their applications to collect on services rendered. If payment is not received by the City within 30 days from outreach, DSD will establish a process to place a "hold" on the customer's record to not allow the customer to obtain any additional permits. Going forward, DSD staff, in collaboration with Finance, will pull the report monthly and review the open jobs to timely close out any that exceed the 180-day window (i.e., expired permits). The revised open job report will be provided to department leadership for potential future workload and revenue earnings. The Pending Fees report will be re-named to "Estimate of Fees for Future Service" or similar name to reduce confusion for any user of this report in the future.				

We are committed to addressing the recommendations in the audit report and the plan of actions presented above.

Sincerely,

Michael Shannon
Director
Development Services Department

3/24/2022
Date

Roderick Sanchez
Assistant City Manager
City Manager's Office

3/24/2022
Date

Craig Hopkins
Chief Information Officer
Information Technology Services Department

29 March 2022
Date

Ben Gorzell
Chief Financial Officer
City Manager's Office

3/30/2022
Date