

17-03 Cash Handling - Part B Cash Procedures and Testing Audit Follow-up

Status of Corrective Actions in Management Responses
 As of February 2018
 Original Report Issuance - July 2017
 Follow-up result: Four of the 27 responses are not yet implemented. Additional follow-up is scheduled.



City Auditor's Office
 Emily E. Kidd, CIA, CGAP
 Internal Auditor

City Manager's Office

Finding	Recommendation(s)	Management Response	Follow-up Status
Citywide Best Practices			
Cash handling controls and procedures were not clear to many employees with access to the City's cash based on observations and interviews during the audit. Most exceptions in the audit are process errors that reflect practices that are noncompliant with the City's documented cash handling procedures in Management Policies and Procedures 407. Without appropriate knowledge and implementation of established internal controls over currency and cash handling, the City's funds are at greater risk of misappropriation.	We recommend the City Manager's Office determine a procedure and process owner to deliver a standard training program for employees responsible for cash handling. Training should be mandatory, be conducted prior to the employee performing cash handling duties, and also ongoing as a periodic reminder of City policies and employee responsibilities. Results of the training should be that employees have sufficient knowledge and understanding of the City's policies and internal controls regarding cash handling.	The City Manager's Office will create a standard training program for employees responsible for cash handling. The training will be mandatory, conducted prior to an employee performing cash handling duties, and recur periodically as a reminder of both City policies and employee responsibilities. The goal of the training will be that employees have sufficient knowledge and understanding of the City's policies and internal controls regarding cash handling. This training will be included in the July 1, 2017 mandatory citywide training set for applicable employees and will recur on an annual basis. The training set is due for completion by August 31, 2017. Completion of the training will be tracked on a monthly basis and reported to supervisory staff in effort to ensure compliance.	Cash handling policy training was assigned to applicable employees through TargetSolutions. One department was granted a waiver until the cash handling policy is updated. At that time, the training will be updated and assigned again.
			Audit Comment to Follow-up: The cash handling policy has not yet been updated as of follow-up date 03/28/18. Additional follow-up on this item is scheduled for August 2018.
Lack of PCI DSS Policy			
Examination of the City of Reno Management Policies and Procedures identified there are no policies addressing Payment Card Industry Data Security Standard (PCI DSS) best practices and standard procedures surrounding credit card data. PCI DSS Requirement 9.10 states, "Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties." Inquiries conducted during the audit identified the lack of training and understanding of PCI standards from employees that handle credit card data. Without appropriate knowledge of and implementation of PCI best practices, credit card data in the City's possession may be compromised.	We recommend the City Manager's Office establish a citywide PCI policy for credit card transactional processing that is based on best practices and make it known to all affected parties.	The City Manager's Office will establish a citywide PCI DSS policy for credit card transactional processing that is based on best practices. By following already established procedures to create a new policy, all affected parties will be notified. The draft policy will be completed by June 30, 2017, with a goal of completing the approval process by July 31, 2017. The City Manager's Office will review the policy on an annual basis to determine if any updates need to be made.	The Department of Information Technology is actively working on researching a PCI policy. It has been determined that a single policy may not be most applicable for the organization. Once the policies are developed, they will be reviewed annually with all City policies.
			Audit Comment to Follow-up: This item has not been resolved as of follow-up date 03/28/18. Additional follow-up on this item is scheduled for August 2018.
System Access Not Removed Timely			
System access to computerized cash receipt systems was not removed timely for individuals no longer employed by the City in multiple departments. A centralized, systematic citywide process could better implement timely access removal when individuals leave City employment. PCI DSS Requirement 7.3 states, "Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties." Without appropriate knowledge of and implementation of PCI best practices, credit card data in the City's possession may be compromised.	We recommend the City Manager's Office establish a citywide employee separation policy and process to include system access removal. It is further recommended the documentation of separation include the date of system access removal.	The City Manager's Office will establish a citywide employee separation policy and process which includes system access removal. The policy will require that documentation of the date of system access removal. The draft policy will be completed by June 15, 2017, with a goal of completing the approval process by July 15, 2017. The City Manager's Office will review the policy on an annual basis to determine if any updates need to be made.	An employee separation policy was adopted 01/08/18. This policy will also be reviewed annually.

Finding	Recommendation(s)	Management Response	Follow-up Status
<p>Access to City Funds</p> <p>The handcart used to collect the parking meter coins and the currency drop box containing parking lot payments do not adequately secure the City's funds. To access the handcart's contents, the wing nut from the top of the handcart is simply removed. There was not a locking device on the handcart. In addition, the key that accesses the parking lot currency drop box's contents is not secured during the drop process. By design, content keys for currency drop boxes are keyed separately from the keys that remove the box from the kiosk to preclude personnel that remove the box from access to the contents of those boxes. Without appropriate preventative internal controls over the access keys, the City's funds are at greater risk of misappropriation. Management Policies and Procedures 407 Section VII.D.1 states, "Access to monies will be limited to as few employees as possible." The current procedure is for the meter technicians to switch-out an empty collection box when they remove the full box from the kiosks; the content/access key is present during the entire box removal process.</p>	<p>We recommend a padlock be secured onto the handcarts used to collect the parking meter funds. In addition, we recommend the meter technicians be precluded from having access to the drop box content keys while outside the vault room and all content access keys be maintained inside the vault room at all times.</p>	<p>Pad locks installed on the coin collection cart. Keys are kept inside the vault room where remain at all times. Measures have been implemented as of May 31, 2017. Both coin collection carts have been retrofitted with locks and are only to be opened inside the vault. Keys will remain in the vault. Drop box content keys will remain in the vault. Measures have been implemented as of May 31, 2017.</p>	<p>02/08/18: Follow-up audit examination of the coin collection cart padlock & keys and drop box content keys that are now maintained in the vault.</p>
<p>Oversight of City Funds</p> <p>A reconciliation of the coin collected at the meters is not conducted. The software system has the ability to produce detailed reports that would allow for a reconciliation of the funds. Without a process to ensure the amount collected was counted and received by the City, the funds are at greater risk of misappropriation. MPP 407 Section VII.F.3 states, in part, "For locations with computerized cash receipt systems ... the computer totals shall be reconciled to the cash receipts to be deposited ..." A reconciliation of the credit card revenues at the meters is being conducted by the Finance Department.</p>	<p>We recommend a reconciliation of the meter coin collections be performed systematically and significant shortages be reviewed.</p>	<p>The Management Assistant will run IPS report to cross reference the counting of the collections. Significant shortages will be reviewed. Measures have been implemented as of May 31, 2017. We are in the process of replacing all non-audit meters with IPS smart meters.</p>	<p>July 2017: All non-audit meters replaced with IPS smart meters. 03/02/18: IPS coin collection report compared to daily bank deposits have been cross referenced with no shortages.</p>
			<p>Audit Comment to Follow-up: The reconciliation recommended was not performed on a systematic and ongoing basis by staff due to a misunderstanding of the recommendation. Discussed the expectation that an ongoing reconciliation be performed by as a standard operating procedure within the department with Public Works management on 03/13/18. Additional follow-up on this item is scheduled for August 2018. Noted a review was performed by staff for January 22-26 upon document request from audit with no significant shortages.</p>
<p>System Access</p> <p>System access to the web-based software IPS is not commensurate with employees' designated duties. Noted two employees that conduct the meter coin drop are assigned access of Manager Role within the system. By assigning access of managerial functions to non management employees, the City's funds are at greater risk of misappropriation. MPP 407 Section VII.A.7 states, "For locations with computerized cash receipt systems, access to programs shall be limited by password to only those programs required to complete designated duties."</p>	<p>We recommend the user role access be adjusted for the employees identified to permit access to designated duties required, but not additional access.</p>	<p>Modify user access to limit users to view only what is necessary to perform necessary duties. Measures have been implemented as of May 31, 2017.</p>	<p>User access remains limited to view only what is necessary to perform duties.</p>
<p>Best Practices</p> <p>Cash handling procedures are not documented for the parking meter and parking lot collection and count process. Establishing written policies detailing cash handling controls is the first step to clarify processes and employee expectations when carrying out their day-to-day functions concerning cash handling. The City's MPP 407 Cash Handling Policy does not include standards for the coin drop and count process. The process owner for the current drop and count process is Public Works. Conducting cash operations without documented process standards is not within best practices for cash handling. Documented internal control procedures, when in use, also assist with departmental succession planning.</p>	<p>We recommend coin drop and count procedures be developed, documented, and communicated to applicable staff.</p>	<p>A parking consultant is scheduled for an on-site visit in June 2017 to develop and establish coin drop and count procedures. Procedures will be in place in the next several months (June – August 2017). Follow established procedures to ensure policies and procedures are being followed correctly.</p>	<p>Parking consultant made site visit in June 2017 and a preliminary findings report was drafted with recommendations to overall parking program. Staff is working with consultant to draft a new contract for establishing Best Practices Manual, which includes developing coin drop and count procedures. Best Practices Manual should be in place by July 2018.</p>
			<p>Audit Comment to Follow-up: Documented procedures for the coin drop and count are not yet completed as of the follow-up date 03/02/18. Additional follow-up on this item is scheduled for August 2018.</p>

Finding	Recommendation(s)	Management Response	Follow-up Status
<p>Internal Controls for Payment Data</p> <p>Credit card information is transmitted through email attachments. The Reno Fire Department Fire Self-Inspection Checklist provides three options for payments from customers, check by mail, credit card by mail, or credit card via email attachment. For payments with a credit card, the form provides blank fields for the credit card information. The completed form is then mailed or scanned, attached, and emailed to the Reno email address provided on the form. The Reno email address is a user group that is received by two City employees. Although one user indicated the emails are deleted once they are processed, the email retention practices of City's Information Technology Unit are that emails are maintained in a repository in the Google cloud environment. Thus, the security of the credit card data is compromised in the transmittal process and the storage of the emails with attachments.</p> <p>The Government Finance Officers Association (GFOA) states, "Credit card acceptance is subject to strong industry security requirements known as Payment Card Industry Data Security Standards (PCI DSS)." And also "Implementation and periodic review of internal controls that address control, confidentiality of data, integrity of data, and other information security issues as appropriate. Internal controls implementation and review should incorporate the current PCI Standards." PCI's Standards indicate organizations accepting payment cards are expected to protect cardholder data and to prevent their unauthorized use. Specifically, PCI version 3.2 Requirement 9.6 states, "Maintain strict control over the internal or external distribution of any kind of media" with media "including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes."</p>	<p>We recommend the option to pay with credit card via email be removed from the verbiage on the Reno Fire Department Self-Inspection Checklist prior to the next batch of mailings and payments by email no longer be considered as a viable payment option by the department. In addition, we recommend the emails containing credit card information be identified and departmental management work with the City Attorney's Office, IT, and the City Clerk's Office to develop a method to safeguard the electronic cardholder data in the City's possession.</p>	<p>This verbiage has been removed from the Reno Fire Department Self-Inspection Checklist as of 4-4-17, immediately after the initial desk audit. Completed as of 4-4-17. Emails containing credit card information were sent to the RFDSelfInspect@reno.gov email. Recipients in this email group, have deleted all received emails regarding the Self-Inspection process, as well as their trash. We contacted the I/T Department and made them aware of the situation to determine if any other deletions in the City's email system needed to occur to ensure that this data could not be accessed. They are confident that these emails can no longer be accessed. Completed. (As of 5-11-17.)</p>	<p>2/12/18 - Fire Department Self-Inspection Checklists no longer have credit card information on the form itself. A separate credit card payment form is mailed with the checklist and emails are no longer accepted with credit card information on them. When credit card information is received for payment, it is secured until process. After processing, credit card payment forms are shredded. This process has been in place since 4-21-17.</p>
<p>Internal Controls for Payment Data</p> <p>Credit card information is not securely stored and is maintained after the business need to retain it has passed. The Reno Fire Department Self-Inspection Checklist provides blank fields for the credit card information to be filled-in by the customer. The data is used by the office assistant when processing payments for those mailed to the administrative offices. The form is then stacked in an open cabinet for additional processing at a later time. During the audit observation, there were hundreds of forms in the cabinet that were backlogged. We were informed that additional processing includes "whiting-out" the credit card information prior to scanning the forms into Documentum for digital retention. After the forms are scanned, they are placed in a secured shred bin for destruction. PCI version 3.2 Requirement 9.5 states, "Physically secure all media" and Requirement 9.8 states, "Destroy media when it is no longer needed for business or legal reasons."</p>	<p>We recommend documented credit card information be placed in the secured shred bin for destruction immediately after payments are processed.</p>	<p>All returned Self-Inspection Checklist forms have had credit card information removed. That credit card information was destroyed (placed in the secured shred bin for destruction). The Checklist has been modified so that credit card information is no longer on the form. Measures were put into place immediately to remove the credit card information on the returned forms. All credit card information was removed from the existing forms by 4-21-17. Credit card information has been removed from all current forms in use. Any forms that are received with credit card information are immediately processed and that information is removed from the form.</p>	<p>2/12/18 - Fire Department Self-Inspection Checklists no longer have credit card information on the form itself. A separate credit card payment form is mailed with the checklist and emails are no longer accepted with credit card information on them. When credit card information is received for payment, it is secured until process. After processing, credit card payment forms are shredded. This process has been in place since 4-21-17.</p>
<p>Security of City Funds</p> <p>The checks mailed to the Fire Department's Administrative office and processed by staff are not endorsed immediately upon receipt as required by City policies. MPP 407 Section VII.C.3 states, "The person opening the incoming mail will restrictively endorse all checks 'For Deposit Only' immediately upon receipt." Inking "For Deposit Only" creates a restrictive endorsement (under the Uniform Commercial Code/ UCC §3-206) and provides another layer of security to ensure the value of the check be paid to the endorsed account. Noted during the observation of departmental processes, the checks were not endorsed until they are prepared for the bank deposit by City Clerk employees rather than immediately upon receipt as stated in the procedures.</p>	<p>We recommend checks be restrictively endorsed upon receipt as stated in the policies.</p>	<p>"For Deposit Only" check endorsing stamps were ordered and received immediately following the initial desk audit. As checks are received by Fire Administration staff they are endorsed immediately upon receipt. Measures were immediately put into place once endorsing stamps were received on 4-7-17. Internal Control – Policies and Procedures – Cash Handling Processes will be updated to reflect this process, as well as training for all Administration staff that open or receive mail.</p>	<p>2/12/18 - Process on-going and adhered to since 4-7-17.</p>
<p>Security of City Funds</p> <p>The cash and checks received in administration's back office are not secured while awaiting deposit. The funds are maintained in an unlocked desk drawer prior to deposit preparation and, while the back office is secured from the public via a key-pad door entry, it is not physically restricted from unauthorized employees. MPP 407 Section VII.D.2 states, "Direct physical access to cash held on City premises can be effectively limited by the use of locked drawers, safes, locked deposit bags, and similar types of protective equipment. Access to such security devices will be physically restricted to authorized personnel only and strictly enforced. Smaller office safes and drop boxes will be permanently bolted to the floor or wall." Without appropriate preventative internal controls over currency, the City's funds are at greater risk of misappropriation.</p>	<p>We recommend the funds be secured in a locked drawer or safe as stated in the policies.</p>	<p>Checks pending deposit, once stamped with the endorsement stamp will be locked in a secured location. Measures were immediately put into place after the initial desk audit on 4-4-17. Internal Control – Policies and Procedures – Cash Handling Processes will be updated to reflect this process; as well as training for all Administration staff that receive checks. RFD – Internal Control – Policies and Procedures – Cash Handling Procedures have been updated – Effective Date May 1, 2017.</p>	<p>2/12/18 - Process on-going and adhered to since 4-4-17.</p>

Finding	Recommendation(s)	Management Response	Follow-up Status
<p>Cash Close-Out Process</p> <p>The close-out procedures involve the cashier comparing the cash on hand to the system's cash total prior to closing out the session without mitigating internal controls in place. The current process is for the cashier to review the system's daily drop total amount for his/her own drawer and compare to the cash on hand in an attempt to balance the drawer prior to closing out the session. After the balance is completed, the cashier then prints the system close-out report, collects the cash on hand, and drops the envelope and paperwork into a safe. This process does not include mitigating internal controls. Per MPP 407 Section VII.F.3 states, in part, "For locations with computerized cash receipt systems, a designated person other than the cashiers shall initiate the daily cash summary program (or its equivalent) at the end of the day." Without internal controls to ensure the amount collected is included in the cash drop, the City's funds are at greater risk of misappropriation.</p> <p>The culture in the department encourages the exact balance of cash drop to the system report. As a result, the overs/shorts are minimal for departmental deposits. Balancing the cash drawer prior to session close-out is not within best practices for cash handling. Also, MPP 407 Cash Handling, states "Overages/Shortages [are] discrepancies noted between the physical count of daily cash receipts and reconciliation to amounts recorded by the cash register or computer summary information. Large discrepancies shall be documented and investigated by supervisory personnel." The financial system includes a separate account designated for overs/shorts. Per an examination of the financial system's over/short report for PRCS for Fiscal Year 15/16, noted just five overages and 12 shortages. During a year of cashiering activity at multiple locations it is reasonable to presume there would be many small dollar amounts of overages/shortages as PRCS cash transactions are a common function of their operations and minor cashiering errors are not uncommon.</p>	<p>We recommend internal controls be identified and implemented for the cashier close-out process. Internal controls may include one or a combination of the following recommended processes: a designated employee other than the cashier initiate the cashier's session close-out prior to the drawer count (a blind drop) to enhance the segregation of duties for cashiering functions, a designated employee other than the cashier reconcile cash dropped by the cashier to the system's close-out report, adjust system access to preclude cashiers from running system report totals, or adjust system access to preclude voids by the cashier.</p>	<p>PRCS will implement the recommendations from the audit. Management has reviewed the recommendations, and compliance will be achieved via the following:</p> <ul style="list-style-type: none"> * Cashiers will no longer print out their drawer reports. A blind drop will be implemented in which the cashier counts the money in their drawer, signs a summary form and drops the money into the safe. * A designated employee other than the cashier will reconcile cash dropped by the cashier to the system's close-out report. * System access will be adjusted to preclude cashiers from running system report totals. * System access will be adjusted to preclude voids by the cashier. * Overages/shortages will be accurately reported. Memos will be written to document justification. Supervisory staff will review mistakes with cashiers at their next shift. Immediately upon training. 	<p>Recommendations have been implemented.</p> <p><u>Audit Comment to Follow-up:</u> Examined the <i>PRCS Cash & Deposit Handling Procedures</i> and noted it details that a blind drop be performed at the end of each shift. No further follow-up required.</p>
<p>System Access</p> <p>System access to the software Active is not commensurate with employees' designated duties. Within the system, each employee is assigned an access level that contains specific permissions. At the time of the audit there were 12 levels within the system. Noted all cashiering levels include the ability to transact voids and refunds allowing non-supervisory staff to transact voids without authorization. Per MPP 407 Section VII.B.3 "All cash register overrings or voids require the authorization and verification of a supervisor or another individual independent of the transaction." Also, MPP 407 Section VII.A.7 states, "For locations with computerized cash receipt systems, access to programs shall be limited by password to only those programs required to complete designated duties."</p>	<p>We recommend the user role access be adjusted to permit access to designated duties required, but not additional access with special consideration given to void and refund permissions.</p>	<p>PRCS will implement the recommendations from the audit. Management has reviewed the recommendations, and compliance will be achieved via the following:</p> <ul style="list-style-type: none"> * System features will be customized by user level so that cashiers cannot do voids or refunds. * User role access is approximately 95% complete. We anticipate the final audit recommendation will be completed within the next 30 days. (As of 06/01/17.) 	<p>Recommendations have been implemented.</p> <p><u>Audit Comment to Follow-up:</u> Examined <i>System Users</i> listing as of 03/05/18. Examined the <i>PRCS Cash & Deposit Handling Procedures</i> and noted it states voids should not be completed by non-supervisory staff. No further follow-up required.</p>
<p>Oversight of System Voids, Overs, and Shorts</p> <p>System voids and overs/shorts are not tracked and analyzed. At the time of the audit, the ability to void was granted for all cashiering user levels, overs/shorts were not consistently documented during the close-out process, and administrative/management analysis of voids and overs/shorts was not conducted. Cash handling best practices include monitoring non-standard cashiering functions including voids and overs/shorts. Tracking and analyzing these types of transactions increases accountability over non-standard transactions and may prevent employees from misappropriating cash payments.</p>	<p>We recommend departmental administration/management track voids, overages, and shortages and analyze for employee or location trends that may indicate misappropriation of City funds.</p>	<p>PRCS will implement the recommendations from the audit. Management has reviewed the recommendations, and compliance will be achieved via the following:</p> <ul style="list-style-type: none"> * Overages/shortages will be accurately reported. Memos will be written to document justification. Supervisory staff will review mistakes with cashiers at their next shift. * System access will be adjusted to preclude voids by the cashier. * If staff makes an error they will let a supervisor know immediately so it can be corrected. If not, then an email will be sent for correction the following day. * PRCS Admin staff will review voids on a weekly basis. Internal policies will be reviewed and updated to reflect new measures. Training will commence after updates are completed within the next 30 days. (As of 06/01/17.) 	<p>Recommendations have been implemented.</p> <p><u>Audit Comment to Follow-up:</u> Examined the system report <i>Revenue Ledger Detail Listing</i> filtered for overages/shortages for January 2018. Noted it was generated by Admin staff on 02/13/18 and all overages/shortages had a timely memo with an explanation for the variance. No further follow-up required.</p>
<p>Timely Financial Reporting</p> <p>The roll-up procedures completed at City Hall are not delivered for processing consistently for timely financial reporting. MPP 407 Section VII.A.8 states, "All cash receipts shall be deposited intact within two business day of receipts." The current timeliness of bank deposits can be improved to streamline financial reporting. Management indicated delays are generally due to the fact that the rollup process is completed by just one employee. When that employee is out of the office processing deposit paperwork is delayed.</p>	<p>We recommend a secondary employee be trained to process the roll-up procedures at City Hall for the department when the primary employee is out of the office for timeliness of financial reporting and succession planning.</p>	<p>PRCS will implement the recommendations from the audit. Management has reviewed the recommendations, and compliance will be achieved via the following:</p> <ul style="list-style-type: none"> * All staff to review and comply with PRCS Cash & Deposit Handling Procedures document on the G: drive. * Daily pickups will be done by Recreation Division admin staff to ensure compliance with M/W/F drop off to PRCS Admin. * Secondary and tertiary employees located in the PRCS Admin office will be trained by Primary employee for financial reporting. Immediately upon training. 	<p>Recommendations have been implemented.</p> <p><u>Audit Comment to Follow-up:</u> Examined the <i>PRCS Cash & Deposit Handling Procedures</i> and noted it includes a secondary employee for roll-up procedures for timely financial reporting. No further follow-up required.</p>

Finding	Recommendation(s)	Management Response	Follow-up Status
System Access			
<p>System access to the software Accela is not commensurate with two of the sampled employees' designated duties. Within the system, each employee is assigned a user group that includes a myriad of specific permissions. We sampled some of the employees' permissions that did not appear to lineup with job function and queried employees' supervisory personnel to determine if the permissions were required for employees' operational duties. Multiple permissions were not needed for the employees' job duties. By assigning additional permissions to employees, the proper functioning of the software and its processes are at greater risk of tampering and unauthorized changes. MPP 407 Section VII.A.7 states, "For locations with computerized cash receipt systems, access to programs shall be limited by password to only those programs required to complete designated duties." Supervisory personnel indicated new employee access is generally requested to mirror another employee that is already set-up with system access.</p>	<p>We recommend the permissions be adjusted for the employees identified to permit access to designated duties required, but not additional permissions.</p>	<p>Staff will adjust the two sampled employees Accela permissions to remove the edit functions and any additional permission not associated with their job duties immediately. Furthermore, we will make those wholesale changes to all other User Groups with the roles, that were given to various employees in those positions within 6 weeks (by end of July).</p> <p>To assure compliance, after Accela support staff alter the permissions they will provide evidence to department management showing these employees' rights within their user groups have been changed. To measure and monitor compliance, Accela support staff will semi-annually (or annually) provide the reports "Accela Access Audit" and "Permission Matrix" to department management. (These will not be run at the same time as the subscription True-up.)</p> <p>The 2 sampled employees Accela access and permissions will be adjusted to those needed for their job duties immediately; the comprehensive change to User Group permissions within 6 weeks.</p>	<p>The employees identified and others in those User groups have been adjusted to remove unnecessary edit functions. In each position type where there is this change, the Access form is required with approval by the division Supervisor.</p> <p><u>Audit Comment to Follow-up:</u> Examined the <i>Accela User Group Permissions</i> and <i>Accela Users - User Groups</i> as of 03/06/18. No further follow-up required.</p>
	<p>In addition, we recommend the permissions for the employee(s) whose access was mirrored be reviewed to determine if access is appropriate.</p>	<p>Accela support staff will no longer mirror Accela access, but rather a new methodology for setting up and requesting users in Accela is being established through a forthcoming Accela Management Policy, setting out business rules. Accela Support staff and CD Managers will develop standards for access based on job title and job duties in order to better refine each user group, such as Development Permit Technicians with the user group functions and roles outlined, and remove any unnecessary permissions from the entire group roles. • Example: Permit Tech roles, Planner roles, and Business License roles, then on a case by case basis those special roles needing edit functions, such as Supervisors or managers authorizing voids, etc.</p> <p>Specific written Permissions - The new access will also have a formalized requesting method requiring that the supervisor of the employee needing access must request access for their employee. (Contained within to be approved Accela Management Policy and Procedure.) Requests must use a predefined questionnaire with criteria, including required job duties in Accela. Approval will also be required by each divisional manager overseeing the particular module being requested. • Example: Business License module access for someone other than business license requires approval by Business Relations Manager, Building Module requires Building & Safety Manager approval, etc.</p> <p>Within 6 weeks the new standards will be defined and begun to be adjusted. (As of 06/07/17.)</p>	<p>The "Accela Access Form" is completed for new employee Accela access requests. Supervisors define the job duties and submit their approval on the form.</p> <p><u>Audit Comment to Follow-up:</u> Examined the <i>Accela Program Management IT Policies and Procedures</i> dated 08/30/17. No further follow-up required.</p>
	<p>Finally, we recommend the process of mirroring employee access when assigning system access be reviewed to determine if it is the most effective way to assign access required for job functions.</p>	<p>Management agrees the mirroring process is flawed. A new methodology for setting up and requesting users in Accela is being established within the to be approved Accela Management Policy and Procedure. Additionally, CD Managers and Accela Support staff will develop standards for access based on job title and job duties in order to better refine each user group, such as Development Permit Technicians with the user group functions and roles outlined, and remove any unnecessary permissions from the entire group roles. To measure and monitor compliance, Accela support staff will semi-annually (or annually) provide the reports "Accela Access Audit" and "Permission Matrix" to department management.</p> <p>Within 3 months (late August) the Policy will be completed. The criteria based questionnaire for access and divisional manager approval are already being implemented for any new Accela account. Compliance with the to be approved Accela Management Policy and Procedure will be required and Accela support staff will semi-annually (or annually) provide the reports "Accela Access Audit" and "Permission Matrix" to department management.</p>	<p>The "Accela Program Management" policy is effective August 30, 2017.</p> <p><u>Audit Comment to Follow-up:</u> Examined the <i>Accela Program Management IT Policies and Procedures</i> dated 08/30/17, the <i>Accela Access Form</i>, and <i>Permissions Matrix</i>. No further follow-up required.</p>
Cash Handling Policies and Procedures			
<p>Cash handling procedures are not documented for the department. Establishing written policies detailing cash handling controls is the first step to clarify processes and employee expectations when carrying out their day-to-day functions concerning cash handling. Conducting transactional operations associated with customer fees without documented process standards is not within best practices for cash handling. Documented internal control procedures, when in use, also assist with departmental succession planning.</p>	<p>We recommend procedures be developed, documented, and communicated to applicable staff; periodic updates to the procedures are also recommended.</p>	<p>Cashiering has been completely transferred to the City Clerk's Office as of February 2017. However, a draft Community Development Cashiering Policy and Procedure for handling and approving voids, refunds, and adjustments has already been developed, and will be approved by CD Director regardless. To be approved July 1, 2017 by the Department Director, and subsequently enacted by staff.</p> <p>Regular communication with the City Clerk's Office, Finance and Accounting staff, and CD divisions will occur, as well as review of the policy annually with updating as necessary. Compliance with the Policy will be warranted.</p>	<p>CD's "Cashiering Policy: Including Corrections, Refunds, Voids by divisions" is effective July 25, 2017. Communication with City Clerk staff is ongoing.</p> <p><u>Audit Comment to Follow-up:</u> Examined the Community Development Management Policy and Procedures titled <i>Cash Policy</i> with effective date 07/25/17. No further follow-up required.</p>

Finding	Recommendation(s)	Management Response	Follow-up Status
<p>Register Keys are not Restricted</p> <p>The cash register and the register keys are available to all cashiers; they are maintained next to the register in Records and in a nearby unlocked drawer in WAU. Register keys can provide an internal control when they are maintained by a supervisory employee that does not function as a cashier. Precluding cashier access to the keys would require the supervisory key holder to be present to access register reports and authorize voids. Per MPP 407 Section VII.A.6, "For locations with no computerized cash receipt system, internal cash register tape/information is inaccessible to cashiers (e.g., keys are maintained by an individual independent of the cash receipt function.)" Also, per MPP 407 Section VII.B.3 "All cash register overrings or voids require the authorization and verification of a supervisor or another individual independent of the transaction."</p>	<p>We recommend the register keys be secured by supervisory personnel to impart the internal controls they were intended to provide such as precluding cashiers from accessing register reports and transacting unauthorized voids.</p>	<p>The register keys will be secured by supervisory personnel in a locked box in the supervisor's office at all times. These measures have already been implemented. (As of 04/18/17.)</p>	<p>This process is still in place.</p>
<p>Close-Out Process</p> <p>The deposits in WAU are being prepared by the cashier and no supervisory presence is in place during the process. Per MPP 407 Section VII.F.1 states, in part, "For locations with no computerized cash receipt system, a designated person, other than the cashiers, shall "Z-out" the register at the end of the day." The procedures at WAU are for the cashier on duty, generally the same cashier that has been transacting throughout the day, to use the register keys to X-out the register and compare the revenues to the cash on hand. The cashier then runs the Z-tape to close out the register at the end of the business day. By running the X-tape and balancing the drawer prior to Z'ing out, the ability to alter the cash prepared for deposit to the funds received in the register increases. The procedures at Records are similar with the exception that a supervisor, not a cashier, runs the close out reports and prepares the deposit.</p>	<p>We recommend the register keys be maintained by supervisory personnel and, at the close of business day, a supervisor Z-out the register.</p> <p>In addition, we recommend the X-report not be run but the register simply be Z'ed-out at the end of the day to ensure a blind drop of the cash on hand.</p>	<p>The register keys will be maintained by supervisory personnel in a locked box in the supervisor's office and a supervisor will handle the closing of the register to Z-out, with the cash handler bearing witness to the count of money for deposit and drawer. A designee will be assigned for both Records and WAU in the event that there are no supervisors on site. These measures have already been implemented. (As of 04/18/17.)</p> <p>The X-report will not be run but simply Z'ed out at the end of the day. This measure has already been implemented. (As of 04/18/17.)</p>	<p>This process is still in place.</p>
<p>Secondary Review of Deposits</p> <p>The deposits in Records and WAU are not being verified by a second individual as is required by policy and as a general best practice for cash deposits. Per MPP 407 Section VII.E.1 states, in part, "The bank deposit must be verified by a second individual that had not collected the cash being deposited." The current procedures are for the cashier on duty in WAU, and a supervisor in Records, to count the cash drawer to its imprest amount of \$100, collect the remaining cash and checks, and place into a clear bank deposit bag. A deposit slip is prepared and placed into the bag and the bag is then sealed. The funds inside the bag are not verified by a second individual prior to their inclusion in the bank deposit.</p> <p>The supervisory review of the cash deposits in Records and WAU is conducted the morning of the next business day and does not include count of the deposited cash and checks inside the sealed bank bag. The review consists of a comparison of the deposit amount on the Z-tape and the amount documented on the close-out form. Per MPP 407 Section VII.F.4, "The Cash Reconciliation Form shall be signed by both the cashier responsible for the cash drawer and the individual completing the reconciliation explained above." The completed close-out forms do include a supervisory signature, however, the current review process cannot attest to the accuracy of the funds within the sealed bag as intended by the policies.</p>	<p>We recommend the prepared deposit funds be verified by a second individual prior to their sealing in the bank deposit bag as stated in the policies.</p> <p>In addition, we recommend the supervisory signature included on the close-out form be an attestation to the verification of the prepared deposit funds.</p>	<p>The prepared deposit funds will be verified by a second individual prior to their sealing in the bank deposit bag. This measure has already been implemented. (As of 04/18/17.)</p> <p>The supervisory signature will be included on the close-out form as an attestation to the verification of the prepared deposit funds. This measure has already been implemented. (As of 04/18/17.)</p>	<p>This process is still in place.</p>
<p>Supervisory Review</p> <p>The supervisory review of the cash deposits in Records and WAU does not include a review of the internal register tape. MPP 407 Section VII.F.1 states, in part, "The cash register tape should be physically reviewed to ensure that the register was not improperly totaled or subtotaled during the day. The register totals shall be reconciled to the cash receipts to be deposited..." Because the register tape is not being reviewed as stated in the policies, it cannot be determined during the supervisory review if the register was improperly Z'ed out since the last deposit. In addition, there are no other logs/documents that identify the sequential Z-reports for WAU. (The Records unit does maintain a log with the sequential Z-reports although, during the audit, the log is not reviewed for gaps in the sequence.)</p>	<p>We recommend the internal register tape be examined during the supervisory review and reviewed for improper totals.</p> <p>In addition, we recommend both locations maintain a document identifying the sequential Z-reports for each business day and they be reviewed by divisional management for gaps in the sequence.</p>	<p>The internal register tape will be reviewed by a supervisor as additional backup for balancing to ensure there are no improper totals. This measure has already been implemented. (As of 04/18/17.)</p> <p>The Records Division is currently in compliance as far as maintaining a 29 daily revenue log identifying the sequential Z-reports for each business day and is being reviewed by divisional management for gaps in the sequence. The WAU daily revenue log has been created to identify the sequential Z-reports for each business day to be reviewed by divisional management for gaps in the sequence. This measure has been implemented for Records since the beginning. This measure has been implemented for WAU. (As of 04/18/17.) The WAU daily revenue log has been created in hard copy and electronic, to identify the sequential Z-reports for each business day to be reviewed by divisional management for gaps in the sequence. An electronic version of daily revenue log has been created as well.</p>	<p>This process is still in place.</p> <p>Audit Comment to Follow-up: Examined the <i>WAU Daily Revenue Logs</i> as of 03/01/18.</p>

Safe Combination is not Limited			
The safe combinations in both Records and WAU are known by employees that are not supervisory personnel. MPP 407 Section VII.D.3 states, in part, "Limit keys to the building, deposit bags, and safe combinations to as few employees as possible, primarily supervisory staff." Limiting access to the safe combinations is a critical component of proper segregation of duties to mitigate the risk of misappropriation of funds. In addition, limiting access to supervisory staff provides a preventative control to ensure supervisors be present when the bank deposit preparation procedures are completed.	We recommend the safe combinations are changed and then known by only supervisory personnel.	The safe combinations for Records and WAU have been changed on April 11, 2017. The safe combinations will be known only by supervisory personnel and a designee in the event that there are no supervisors available on site. This measure has already been implemented. (As of 04/18/17.)	Corrective action taken 4/11/2017 with combinations changed.
Internal Auditor's Note: The audit recommends the safe combination be limited to supervisory personnel only to strengthen the segregation of duties and provide a preventative control over the cash maintained in the safes. However, management responses indicate they have provided access to a designee in the event there are no supervisors available. The designated employee is nonsupervisory and processes cash transactions during daily operational duties. By allowing a single employee extended duties, the preventative controls recommended by the audit are no longer intact and the risk of misappropriation of City funds increases.	Management's response to this exception does not provide an acceptable level of internal controls and residual risk remains. Executive management and Internal Audit further recommends the safe combinations be changed and known only by personnel not involved in daily cash operations, preferably only supervisory personnel.	The Safe combinations for Records and WAU have been changed on April 11, 2017. The safe combinations will be known only by supervisory personnel and designees, in the roles of Management Analyst and Accounting Assistant, in the event there are no supervisors available on site. These roles do not process cash transactions during daily operations. This measure will be implemented on July 12, 2017.	Corrective action taken 7/12/2017 with combinations changed. <u>Audit Comment to Follow-up:</u> Examined the invoices for two combo changes from the lock vendor dated 04/11/17 and 07/12/17.
Check Endorsement			
The checks mailed to PD and processed by Administrative Services staff are not endorsed immediately upon receipt as required by City policies. MPP 407 Section VII.C.3 states, "The person opening the incoming mail will restrictively endorse all checks 'For Deposit Only' immediately upon receipt." Inking "For Deposit Only" creates a restrictive endorsement (under the Uniform Commercial Code/ UCC §3-206) and provides another layer of security to ensure the value of the check be paid to the endorsed account. Noted during the observation of departmental processes, the checks were not endorsed until they are prepared for the bank deposit rather than immediately upon receipt as stated in the procedures.	We recommend incoming checks be restrictively endorsed upon receipt as stated in the policies.	The incoming checks will be restrictively endorsed upon receipt before being placed in the safe/vault as stated in the policies. This measure has already been implemented. (As of 04/18/17.)	This process is still in place.
Safeguarding of City Funds			
The internal controls and documents in use cannot identify if there are any missing deposits for Records and WAU. The current procedures are for the sealed bank deposit bags in those areas to be placed in the safe until they are either picked up or delivered to the Administrative Services Manager. The pick-up/delivery is not on a set schedule nor are the bags "signed off" as delivered on a tracking document. The Administrative Services Manager prepares one bank deposit for all three PD transactional areas for pick up by the armored car service once per week. The bags collected at Records and WAU are not reviewed to determine if there was one prepared for every day the business units collected cash. Because the Records unit does not always conduct cash transactions on Fridays, a straight count of the number of bags could be inconsistent. To identify if any missing deposits occurred for due diligence, Internal Audit reviewed the financial system's Revenue Ledger Detail Listing report for any gaps in deposits for business days for both PD divisions for two sample months and noted four business days without deposits. Examined the daily close-out documentation in PD for the dates identified and, per examination of the sequence of the Z-reports, noted for three of the business days without deposits the unit did not collect cash. One of the business day's revenues was posted to the following date in the financial system. There were no missing deposits for the months reviewed. Current procedures are not within best practices for cash handling. Without a comprehensive review of the Z-reports generated by the cash registers, a Z-report could be run and its associated cash removed from the deposit process without management's knowledge. Also, without a tracking document identifying staff that is responsible for the deposit bags as they move to different areas within PD, pinpointing staff responsible for the funds is not possible.	We recommend that a process be implemented to identify all business days with cash transactions in Records and WAU and the document noted in the recommendation for Finding 21 be reviewed to ensure there are no gaps in the sequence of the Z-reports. Together, these processes could identify any missing deposits from the divisional units. In addition, we recommend the department implement a tracking document for all deposits received in the Administrative Services office to identify where prepared deposit bags are at all times.	Identify all business days with cash transactions in Records and WAU and record that information on the electronic log to ensure there are no gaps in the sequence of Z-reports. This measure has already been implemented. (As of 04/18/17.) The Department has implemented an electronic log tracking document for all deposits received and then verified through the Administrative Services to identify where prepared deposit bags are at all times. This measure has already been implemented. (As of 04/18/17.)	This process is still in place. <u>Audit Comment to Follow-up:</u> Examined the <i>RPD Records & WAU Daily Revenue & Deposit Log</i> (the electronic tracking log) as of 03/01/18.
Fees and Charges Listing			
Examination of the Adopted Fees and Charges FY 16/17 indicates a fee for criminal sealings is charged by PD. Per an examination of PD revenue documents during the audit scope, no criminal sealing fees were collected. Upon inquiry with PD management, audit was informed that the department does not collect this fee for the criminal sealings service because they were instructed by the City Attorney's Office that charging this fee is not permitted by law. Thus, the Adopted Fees and Charges FY 16/17 approved by Council does not reflect actual fees collected by the Police Department. Per discussions with the City Attorney's Office, they have determined that a Police Department service charge to process criminal sealings is not permitted by law.	We recommend PD management communicate the need to remove this service fee from the Adopted Fees and Charges listing prior to the adoption of the FY 17/18 budget and associated fees.	The management will communicate the need to remove the criminal sealing fee from the Adopted Fees and Charges listing prior to the adoption of the FY 17/18 budget and associated fees. This measure will be taken as soon as the proposed fee schedule is received.	This has been completed. <u>Audit Comment to Follow-up:</u> Examined the <i>FY 17/18 Adopted Fees and Charges Listing</i> for PD fees.

<p>Deposit Timeliness</p> <p>Bank deposits are not consistently prepared in a timely manner. Internal Audit examined the armored car pick-up log for a nine month period during the audit scope and reviewed for timeliness. Noted most of the 30 deposits were prepared and picked up at weekly intervals. However, five were at two week intervals, two at three week intervals, and one was not prepared and picked up for four weeks. In all, 27% of the deposits reviewed were completed at intervals greater than one week. MPP 407 Section VII.A.8 states, "All cash receipts shall be deposited intact within two business day of receipts." While this policy is slated to be adjusted to permit weekly deposit at PD, the current timeliness of bank deposits can be improved to better secure funds and streamline financial reporting. Management indicated delays are generally due to the fact that the deposit preparation is completed by just one employee. When that employee is out of the office the deposits are delayed.</p>	<p>We recommend the bank deposits be prepared and picked up consistently on a weekly basis.</p> <p>In addition, we recommend a secondary employee be trained to prepare the deposit for the department for timeliness and succession planning.</p>	<p>The bank deposits will be prepared and picked up consistently on a weekly basis. This measure has already been implemented. (As of 04/18/17.) A secondary employee of the Administrative Services staff will be trained to complete the weekly deposit preparation and pick up in the absence of the Administrative Services Manager.</p> <p>A secondary employee will be trained to prepare the deposit for the department for timeliness and succession planning. This measure has already been implemented. (As of 04/18/17.)</p>	<p>This process is still in place.</p>
<p>Cash Handling Policies and Procedures</p> <p>Departmental cash handling policies are not documented for the Police Department. Per interviews with departmental personnel, a policy was located in the departmental shared-drive. However, the policy has not been updated since 1992 and do not reflect actual procedures in place during the audit observations. Establishing written policies detailing cash handling controls is the first step to clarify processes and employee expectations when carrying out their day-to-day functions concerning cash handling. The effect of no updated policies and a lack of training on cash handling policies is a poor internal control environment that does not adequately secure City funds.</p>	<p>We recommend departmental cash handling procedures be developed, documented, and communicated to staff with cash handling duties. Periodic updates to the procedures are also recommended.</p>	<p>The department cash handling policies are documented however not updated. The department cash handling procedure will be updated periodically. The department is in the process of updating the cash handling policy. The policy will be completed within three months of the final report. The Administrative Services Manager will create a procedural document to outline the cash handling responsibilities within the Administrative Services area.</p>	<p>This has been completed.</p> <p><i>Audit Comment to Follow-up: Examined the Reno Police Department Cash Handling Policies & Procedures dated 04/07/17.</i></p>