OHIO AUDITOR OF STATE
KEITH FABER

88 East Broad Street, 5th Floor
Columbus, Ohio 43215-3506
(614) 466-3402 or (800) 443-9275
CentralRegion@ohioauditor.gov

MANAGEMENT LETTER

City of Shelby
Richland County
43 West Main Street
Shelby, Ohio 44875

To the City Council:

We have audited the financial statements of the City of Shelby, Richland County, Ohio, (the City) in accordance with *Government Auditing Standards*, as of and for the year ended December 31, 2018, and have issued our report thereon dated September 24, 2019; wherein we noted the City adopted new accounting guidance in Governmental Accounting Standards Board (GASB) Statement No. 75, *Accounting and Financial Reporting for Postemployment Benefits Other than Pensions*, and restated January 1, 2018 net position due to a capital asset appraisal.

Government Auditing Standards require us to report significant internal control deficiencies, fraud, (including noncompliance with laws and regulations), and also abuse and noncompliance with contracts and grant agreements that could directly and materially affect the determination of financial statement amounts. We have issued the required report dated September 24, 2019, for the year ended December 31, 2018.

2 CFR Part 200 subpart F requires that we report all material (and certain immaterial) instances of noncompliance, significant deficiencies, and material weaknesses in internal control related to major federal financial assistance programs. We have issued the required report dated September 24, 2019, for the year ended December 31, 2018.

We are also submitting the following comments for your consideration regarding the City's compliance with applicable laws, regulations, grant agreements, contract provisions, and internal control. These comments reflect matters that do not require inclusion in the *Government Auditing Standards* or Single Audit reports. Nevertheless, these comments represent matters for which we believe improvements in compliance or internal controls or operational efficiencies might be achieved. Due to the limited nature of our audit, we have not fully assessed the cost-benefit relationship of implementing these recommendations. These comments reflect our continuing desire to assist your City but are only a result of audit procedures performed based on risk assessment procedures and not all deficiencies or weaknesses in controls may have been identified. If you have questions or concerns regarding these comments please contact your regional Auditor of State office.

NONCOMPLIANCE FINDINGS

1. Federal Uniform Guidance Policies

Implementation of policies is essential in ensuring compliance with federal grant requirements. Lack of policy implementation could result in noncompliance with federal UG requirements. The Code of Federal Regulations (CFR) requires written policies for the requirements outlined below:

NONCOMPLIANCE FINDINGS
(Continued)

1. Federal Uniform Guidance Policies (Continued)

- 200.302 (b)(7) - Written procedures for determining the allowability of costs in accordance with Subpart E - Cost Principles of this part and the terms and conditions of the Federal award.
- 200.302 (b)(6) - Written procedures to minimize the time elapsing between the transfer of funds.
- 200.318(c)(1)-(2) - Written procurement policies for employee conflicts of interest and for organizational conflicts of interest.
- 200.320 (d)(3) - Written policies for selection and awarding of competitive contracts.
- 200.319(c) - Written policies for minimum evaluation criteria for bids and proposals.

As of December 31, 2018, the City did not formally adopt any of the federal written policies listed above.

Failure to have formal written policies and procedures in place could result in noncompliance with federal grant requirements.

We recommend the City adopt written policies over its controls and procedures required by the Code of Federal Regulations.

2. Timely Deposits

Ohio Rev. Code § 9.38 states a person who is a public official other than a state officer, employee, or agent shall deposit all public moneys received by that person with the treasurer of the public office or properly designated depository on the business day next following the day of receipt, if the total amount of such moneys received exceeds one thousand dollars. If the total amount of the public moneys so received does not exceed one thousand dollars, the person shall deposit the moneys on the business day next following the day of receipt, unless the public office of which that person is a public official adopts a policy permitting a different time period, not to exceed three business days next following the day of receipt, for making such deposits, and the person is able to safeguard the moneys until such time as the moneys are deposited. The policy shall include provisions and procedures to safeguard the public moneys until they are deposited.

We noted 9.8% of utility receipts (5 out of 51 selected), 93% of income tax receipts (13 out of 14 selected), and 1 CPR training receipt selected, which were not timely deposited with the Director of Finance by the next business day following the day of the receipt. We additionally noted the City has not established formal cash collection policies and procedures.

Failure to implement formal written policies and procedures over the cash collections process and to deposit receipts timely increases the risk of City funds being lost, misappropriated, or improperly posted, and these errors going undetected by management.

We recommend the City Council implement formal written cash collection policies and procedures over classification and posting of receipts, safeguarding receipts, and depositing timely in accordance with State statute.

RECOMMENDATIONS

1. IT – Logical Access Controls

Logical access controls are necessary to help ensure access is restricted to only those individuals who require such access to perform their job functions. Security or system configuration capabilities should be used to restrict users with administrative access to a small number of users with direct responsibility for the system. In addition, the use of password parameters governing password expiration intervals is a key component in helping to ensure only authorized individuals have knowledge of their user account name and password.

Network Level

The City uses Windows Active Directory (AD) to restrict user access to their City Hall network. City Hall network access is required to access the financial and income tax applications. While password protected accounts are required at the AD level, the following issues were noted:

- A high level account has a password set to not expire and the password was not changed during the audit period.

When password changes are not required for all user accounts, there is an increased risk the access provided may not be secure and consistent with management's intentions. In addition, when audit and event log policies are not defined for the specific needs of the organization, and audit logs are not reviewed on a regular basis for security violations, the risk of undetected break-in attempts increases.

Financial Application

The City's financial application is used as the primary software to record general ledger, purchase order, and accounts payable transactions. Although access is password protected, the following issues were noted:

- For each module in the application (general ledger, purchase order and accounts payable), all four user accounts had administrative access. This access allowed the users to view and change each other's password. During field work, administrative access was modified and limited to one individual.
- For the purchase order module, accounts created specifically to assign department information to purchase orders had read/write ability. These accounts were not intended to have this access. In addition, the passwords for these accounts appeared to be the same. During field work, access to these accounts was changed to no access.

Granting account access beyond assigned responsibilities increases the risk that this access could be used inappropriately. If access is obtained or inappropriately used, these unauthorized users could create or alter financial transactions that could affect the financial statements.

Utility Billing Application

The City's utility billing application is used for the calculation and tracking of water, sewer and electric consumption. Two utility billing clerks appear to have administrative rights to the application.

The provision of administrative access to individuals who do not have direct supervision responsibilities increases the risk that this access could be used inappropriately. If access is obtained or inappropriately used, these unauthorized users could create or alter financial transactions that could affect the financial statements.

RECOMMENDATIONS
(Continued)

1. IT – Logical Access Controls (Continued)

Municipal Court - Application Level

Access to the Municipal Court's application system is restricted with the use of password protected user accounts; however, the following issues were noted.

- A high level account has a password set to not expire and the password was not changed during the audit period.
- The 30 day password expiration policy, applicable to user accounts, was turned off during field work. The policy appeared to be working during the audit period.
- No lockout policy is in place to prevent unauthorized users from attempting logon attempts.

When password changes are not required for all user accounts or password change intervals and lockout policies are not defined, there is an increased risk the access provided may not be secure and consistent with management's intentions. These conditions may result in an unauthorized individual gaining access to the system and accidentally or intentionally deleting or altering sensitive court or financial data.

The City should implement or perform the following logical access controls:

- Enforce periodic password change procedures for all of the AD user accounts. If administrative accounts are needed for other background processes, periodic manual password changes should be applied.
- Review account access to the financial and utility billing applications to determine if the access provided is commensurate with the account owner's job function.
- The Municipal Court should enforce periodic password change procedures for all accounts and create lockout policies for all users.

2. IT – Disaster Recovery Planning

The creation and use of a comprehensive, disaster recovery plan minimizes the risk of loss of data and minimizes the risk that computer operations important for the functioning of the City will not be restored in a timely, cost effective manner after a disastrous event.

To address these risks, the departments of Finance, Income Tax and the Municipal Court create backups on a daily basis and store the backups in secure locations. In addition, application vendor support has been secured by these departments which could be used to aid in the restoration of computing resources if a disastrous event should occur. Although these controls have been established, the departments mentioned above have not created a disaster recovery plan to help coordinate the materials and personnel necessary to restore the other aspects of their operations not covered by vendor support.

Without a comprehensive disaster recovery plan, the departments of Finance, Income Tax and the Municipal Court could incur additional costs and experience additional down time in addressing issues that had not been considered by management. These delays could extend the recovery periods beyond those acceptable by their management.

The departments of Finance, Income Tax and the Municipal Court should create disaster recovery plans for their departments to address typical recovery issues that would not be covered by existing vendor application support.

RECOMMENDATIONS
(Continued)

2. IT – Disaster Recovery Planning (Continued)

At a minimum, the plans should address the following:

- Hardware, software and communication needs for processing at the alternate site, as well as develop a priority list for application processing.
- Identify key personnel necessary for processing at an alternate site. Establish training for the key personnel and allow for the periodic testing of the transfer of processing to the alternate site.
- Establish a manual backup process to bide the organization over to the point that crucial systems can be recovered. The backup process should address personnel, hardware and software requirements as well as the manual flow of paper transactions through the necessary authorization trail.

Once developed, the plan should be tested to ensure its applicability, and reviewed annually to ensure it is up to date; reflecting the current operations of each office.

3. IT - Anti-Virus Software – Municipal Court

The implementation of a security framework supported by processes and the deployment of tools is imperative in helping to minimize the risks that could compromise the integrity and security of information systems. Anti-virus software, which is used to prevent, detect, and remove malware, is one tool, that when implemented correctly, helps to maintain the integrity and security of information systems.

The most efficient implementation of anti-virus software is to use a centrally managed solution. With a centrally managed solution, management can ensure computers are updated with new definitions on a regular basis. In addition, the licensing and scheduling of regular scans can be more efficiently controlled through a centrally managed solution.

The Municipal Court is not using a centrally managed anti-virus software. The lack of centralized control over anti-virus software increases the risk the Municipal Court's network and information systems is not adequately protected from viruses, which could lead to significant downtime and/or data loss.

The Municipal Court should consider installing anti-virus software that can be centrally managed and is appropriately licensed. Controls should also be implemented to help ensure the anti-virus definitions are up-to-date and scans are occurring on a regularly scheduled basis.

4. IT - File Access Permission

To help reduce the risk of unauthorized access and maintain data and application integrity, organizations should restrict access to their computer systems, files, and data. Write, delete, and modify permissions should only be granted where necessary and required to perform processing.

The City uses the security provisions of the windows server operating system to protect the database files of its critical applications. The file access permissions for two of the audit significant servers were found to potentially permit all domain users in their City Hall directory full access to the database files.

RECOMMENDATIONS
(Continued)

4. IT - File Access Permission (Continued)

Granting excessive access to critical application folders and files increases the risk that users will intentionally or unintentionally use this access to alter application database files. Alteration of these files could affect transaction reliability and application function.

The City, in consultation with the application vendor and IT consultant, should review the application database file permissions for the financial and income tax applications. Access to application database files should be limited as much as possible to reduce the risk of intentional or unintentional alteration.

5. IT – Security Administration – Municipal Court

Security management policies and procedures help to ensure computer resources are appropriately provided to management approved users. Security management policies include on-boarding procedures to confirm initial user access is appropriate and continuing review of user access for appropriateness.

The Municipal Court has informal on-boarding policies to ensure new accounts are authorized and have appropriate access. One account was enabled during the audit period for a user who no longer works for the Municipal Court. An explanation for why the account was enabled was not provided. The account was disabled during field work.

When user maintenance policies are not formalized there is an increased risk all the steps necessary to correctly add, change, or remove user access may not be consistently followed or grant access in excess of the access intended. If access is inappropriately obtained or inappropriately used, unauthorized transactions could be generated affecting the financial statements.

The Municipal Court should develop formal user security management and administration procedures to ensure all new accounts have proper management authorization documentation. This will ensure the access of new accounts is appropriate.

We intend this report for the information and use of the City Council, finance committee, and management.

Keith Faber
Auditor of State

Columbus, Ohio

September 24, 2019