SCHNEIDER DOWNS

Big Thinking. Personal Focus.

September 26, 2018

Ms. Tracy L. Bradford
C/O City of Hilliard
3800 Municipal Way
Hilliard, Ohio 43026-1696

On behalf of Schneider Downs & Co., Inc. (Schneider Downs), we thank you for the opportunity to perform a review of the business and accounting practices of the City of Hilliard. The accompanying report is to provide you with observations of the processes, controls and policies of the City of Hilliard.

Work performed was conducted in accordance with the *Statements on Standards for Consulting Services of the American Institute of Certified Public Accountants*. This review did not constitute an audit of financial statements or other attestation engagement in accordance with generally accepted auditing standards. This report has been prepared for use by the City of Hilliard management and council.

Again, we thank you for giving us the opportunity to be of service to you and we look forward to assisting you in the future. If you have any questions, please call me at (614) 586-7257.

Very truly yours,

Donald R. Owens
Shareholder
Risk Advisory Services

Schneider Downs & Co., Inc.
www.schneiderdowns.com
PrimeGlobal
An Association of Independent Accounting Firms

One PPG Place, Suite 1700
Pittsburgh, PA 15222
TEL 412.261.3644
FAX 412.261.4876

65 E. State Street, Suite 2000
Columbus, OH 43215
TEL 614.621.4060
FAX 614.621.4062

CITY OF HILLIARD

Business and Accounting Practices Review

September 26, 2018

SCHNEIDER DOWNS

Big Thinking. Personal Focus.

www.schneiderdowns.com

Table of Contents

I. Background

The City Hall of Hilliard, Ohio is located at 3800 Municipal Way, Hilliard, Ohio 43026. The City of Hilliard (City) is made up of the Hilliard Mayor's Court and Clerk of Courts Office, Hilliard Police Department, Hilliard Recreation and Parks, Department of Economic Development, Land and Buildings Department, IT and Communications Department, Finance Department, and Human Resources Department. These departments function to manage the City's legal, financial and maintenance needs.

II. Objectives and Scope

Based on a meeting held with Ms. Bradford, Mr. Delande and Ms. Baxter on March 7, 2018, it was requested that Schneider Downs & Co., Inc. (Schneider Downs) recommend the consulting services that should be performed to verify that appropriate controls are in place to effectively safeguard the City's funds and assets.

From our understanding, this encompassed the following areas of review:

a. Safeguarding of funds received from revenue sources;
b. Safeguarding of funds disbursed to vendors and other parties;
c. Vendor selection, approval and setup;
d. Contract management that includes bids, awards and contract management oversight;
e. Asset management/safeguarding and accountability;
f. Investment management; and
g. System access security and assessing segregation of duties for the systems that are utilized to perform these functions.

III. Approach

Schneider Downs was engaged to perform a review of the City, evaluate current processes and identify opportunities for efficiency and improvement. As part of our review, we interviewed personnel, reviewed documentation and observed practices associated with the following: receipt of payments, disbursements of payments to vendors, payroll disbursements, issue of citations, physical security of seized property and evidence, compensation and raises, and accounting journal entries.

Schneider Downs met with the City's management to agree on the processes and functions in scope for this review. Once the processes were defined, Schneider Downs met with the City's management and key personnel within each of the following groups (function/position):

a. Mayor/Commissions
b. Mayor/City Clerk
c. Mayor/Clerk of Courts
d. Department of Economic Development/Economic Development Director
e. Department of Law/Law Director

f. Department of Communications & IT/Communications Director
g. Division of Building/Service Director
h. Division of Engineering/Service Director
i. Division of Service/Service Director
j. Lands and Building/Lands and Building Director
k. Division of Parks and Recreation/Recreation and Parks Director
l. Department of Finance/Finance Director
m. Department of Tax/Deputy Finance Director
n. Human Resources/Human Resources Director
o. Division of Police/Safety Director

We conducted interviews to assess which of the in-scope processes are performed by each function; reviewed each process to determine the critical risks that would prevent successful completion; reviewed how the processes are executed from initiation through end state; and, the controls that are performed to mitigate the critical risks.

We developed process documentation (process flowcharts and process narratives) for each process reviewed, and gained an understanding of the processes and the controls in place. We developed a risk and control matrix to assess whether the risks are sufficiently mitigated by existing controls and identified where gaps exist (where risks are not sufficiently mitigated by existing controls). The key systems used to execute the in scope processes were identified and access security has been assessed.

We performed a review to assess whether controls are sufficiently designed to mitigate the critical risks that they are intended to control. This involved a review of control documentation with the control performers. We will present the results of the assessment with the process owners to confirm their understanding of the control design exceptions observed and make recommendations for enhancement.

We assessed the entire lifecycle of how user access is securely managed across key systems and their related databases and operating systems. Specifically, we evaluated the processes used to create and delete user accounts (e.g., end user, privileged, guest and vendor), manage ongoing account and permission changes, and track policy compliance. We assessed the critical user roles held by the respective user accounts, along with the permissions assigned to each role, where possible, for appropriate segregation of duties (SOD) and compatible system access in accordance with user job duties.

IV. Observations and Recommendations

The following are recommendations for enhancing the business and accounting practices that were reviewed as part of this engagement.

1. Clerk of Courts - Ticket and Fees for Court

A monitoring control is not in place to assess the volume and appropriateness of credits and write-offs of fees and other transactions executed by the Clerk of Courts, Building and Engineering, and Recreation and Parks Departments. A lack of independent review and/or monitoring of credits, voids, and write-offs increases the difficulty of detecting and identifying fraudulent activity.

Recommendations: The Finance Department should coordinate with the Clerk of Courts to obtain appropriate reporting of adjustments (voids and credits) at least on a monthly basis to evaluate the propriety of adjustments and assess trends.

2. Clerk of Courts - Physical Access

There is no formal policy in place with respect to identifying the specific housing of confidential or sensitive information to ensure that access to offices that contain confidential or sensitive information is restricted to the appropriate parties only.

Recommendations: The Clerk of Courts should develop a policy specifically stating which offices will house specific types of confidential or sensitive information; who will be authorized access to these offices; and under what conditions access is approved. Identify which offices maintain confidential/sensitive information and determine which parties have access to these offices. Any party that has access to offices that maintain confidential or sensitive information should be held accountable for its contents and who has access to the offices.

Management Response: Per inquiry with the Law Director, the Clerk of Courts office knows who has access to the Clerk of Courts office and who has a key FOB to access the main Clerk of Court's office. Many case files have confidential and sensitive information in them. There are only two offices; files would be located in the Clerk of Courts office if she is working on something with the file. After the Clerk of Courts is finished with the file, it is placed back into the main Clerk's office.

3. Finance - Credit Card Usage

There is not a formal accountability for the City credit card transactions or the ability to trace the individuals that use the credit card. Currently, there are two credit cards in use: one for the Finance Department that is also used by IT & Communications, and one for the Police Department. The credit card can be used by any individual that knows the credit card number or has access to the credit card. A lack of individual accountability for transactions can lead to undetected, unauthorized usage.

Recommendations: In order to prevent the risk of unauthorized usage and to provide accountability and monitoring of transactions, we recommend that the City's credit cards be assigned to individuals rather than a department.

Management Response: In order to use a City issued credit card, there must be a purchase order in place prior to the purchase being made. A signed receipt is also required to be given to the Finance Department after purchase. Currently, most purchases are used by obtaining the credit card number from the Finance Director, but individual credit cards will be considered in lieu of department credit cards. There will be a credit card policy in place that must be signed by all individuals using their City issued credit card. The Finance Director will determine the individuals necessary to have a credit card in their name, as well as the credit limit.

4. Finance - Segregation of Duties

For each revenue source system (Incode, RecTrac, and TOPS), segregation of duty conflicts exist. The department that owns the application is the administrator of the system and can assign privileges at the user level as needed. Users have also been assigned duties that may be considered conflicting (i.e., the ability to record transactions, handle funds received, and record void or credit transactions). Conflicting assigned duties may allow individuals an opportunity to commit undetected fraud.

Recommendations: In order to mitigate this risk, it is recommended that the Finance Department, as an independent function, reviews system reports showing the adjustments recorded each month (e.g., voids and credit transactions) to verify the validity of the transactions and to identify unusual activity or trends.

Management Response: Monthly, the Finance Department will receive reports from various departments along with any adjustments or write-offs such as voids and credit transactions. The Finance Department will review these reports against their own revenue reports and record variances, such as timing differences, between the two.

5. Finance - Accounting for Uncollected Revenue Earned

Revenue due the City that has been earned, but not collected, is not formally monitored to ensure proper tracking and collection is performed. Reliance is placed on offline processes due to the recording of revenue on a cash basis. As a result, there is limited visibility of these revenue and collection opportunities that may result in revenue or funds not being collected or recorded.

The City operates on a cash basis accounting system, and no formal tracking of accounts receivable exists. The lack of monitoring for these revenues provides opportunity for the revenue to go uncollected.

Recommendations: Since the City records revenues on a cash basis, the Finance Department should develop a monitoring process to track all open receivables that have not been recorded to ensure that each department is effectively collecting and addressing the receivable activity.

Management Response: The Finance Department is currently seeking software that will tie into CMI to record all invoices and receivables for formal tracking of uncollected revenues.

6. Finance - Requisition and Purchase Orders

There is no formalized process for new vendor setup. A new vendor typically has a quote on letterhead, or if they are an independent contractor the Federal ID number is required.

Recommendations: A policy should be implemented surrounding the requisition and PO process that explicitly states the requirements for new vendor setup. Prior to business being done the City should require a W-9 for all new vendors, and that a new Vendor Form be completed by the department requesting the new vendor. If possible, all personnel might be required to disclose any personal relationships to a new vendor (arms-length transactions).

Management Response: Per inquiry with Tracy Bradford, obtaining a W-9 for all new vendors and new vendor form completed by the requesting department would be a policy the Finance Department will implement going forward, following the conclusion of the report. Finance will work on obtaining any personal relationships to vendors currently on the approved vendor masterfile, as well as new vendors going forward.

7. Finance - Requisition and Purchase Orders

All Finance Department personnel have access to add and delete users, and change privileges and thresholds within the CMI system. A Lack of application control configuration setting can lead to inappropriate approval of purchase requisitions and purchase orders.

Recommendations: The following process enhancements are recommended:

a. System administration and user provisioning would be best executed by IT & Communication, which is independent of the production activities, rather than the department that owns the application and performs the daily production transactions. For best practices, user privileges should be designated on a user role basis to segregate conflicting duties, and access by employees should be assigned to the respective user roles.

b. Where duties cannot be effectively segregated, monitoring should be implemented to assess transactions for inappropriate activity.

Management Response: The IT Department will add and delete users, and change privileges and thresholds within the CMI system.

8. Human Resources - Payroll

Payroll policy states that directors "should" not approve their own time sheets. However, the access privileges within the Right Stuff (time reporting application) allows the Directors the capability to approve their own time. A lack of application control configuration setting can lead to inappropriate approval of payroll.

Payroll changes are reviewed and verified by the payroll processor that inputs the payroll changes rather than an individual or function separate than the payroll processor. This may result in inappropriate payroll activity that is not detected. A lack of independent review can result in undetected and inappropriate payroll activity.

The Payroll processor validates completeness of payroll changes in CMI by agreeing the source documentation requesting or approving the change to the Payroll Detailed Work Register (Payroll Register). The Payroll Register shows the full payroll rather than just the changes for the pay period, making it difficult for a reviewer to detect and validate the changes made that did not have a valid source document. A lack of a system report increases the risk of incomplete and inaccurate payroll data.

Recommendation: The following process enhancements are recommended in order to reduce the risk of payroll errors or fraudulent payroll activity:

a. Revise the application security privileges to prevent directors from approving their own time reports within the Right Stuff system.

   Management Response: Per the Human Resources Director, security privileges have been revised to prevent directors from approving their own time reports within the Right Stuff system.

b. Payroll changes should be reviewed and validated by an individual or function separate from the person that executes the bi-weekly payroll.

   Management Response: Per the Human Resources Director, moving forward, the Finance Department will review and validate any payroll changes prior to the Human Resources Department inputting the changes into the CMI system.

c. It is recommend that a payroll change report be developed to show all changes made to payroll during the pay period (new hires, terminations, pay rate changes, and other deduction and tax changes) to enable a complete validation of pay period changes.

Management Response: Per the Human Resources Director, HR is in the process of developing an in-house payroll change report and saving it on the shared drive in which only HR will have access. The Payroll Specialist will create the document and, before any payroll change is made, the Finance Department will verify the changes. This process will go into effect upon the placement of the payroll change report on the shared drive and restricted access is established.

9. Human Resources - Mandatory Vacation

Mandatory vacation is not required by the City's hourly, salaried, union, non-union, full-time, part-time, or temporary employees.

Recommendation: The City implement a policy that all full-time employees, whether union or non-union, hourly or salaried, take a mandatory one week (5 consecutive business days) vacation.

Management response: Response not yet received.

10. Human Resources - Use of City Vehicles

The City did not have a policy regarding the use of City vehicles and equipment at the time of the audit. However, a *Vehicle and Equipment Use Policy* was approved August 6, 2018.

Recommendation: The policy must be implemented and adequately monitored to ensure that the policy is being enforced and adhered to by all department and division management.

Management Response: Response not yet received.

11. Land and Buildings - Fixed Asset Retirements and Additions

There is no independent, periodic review of the City's fixed assets that ties back to the fixed asset register.

Recommendation: Finance should work with the Land and Buildings Department (and other departments as necessary) to develop a process for identification of assets that are being added or retired to ensure that accurate and complete updates are made to the Fixed Asset Register and revisions are appropriately made to the asset net book values.

Management Response: A *City of Hilliard Fixed Asset Policy, January 1, 2004* has been adopted by the City. Per the Finance Director, the Finance Assistant plays an active role in day to day transactions and inquiries to include reminding each department when to review their fixed asset inventories for accuracy. Each department is aware of policy thresholds and daily transactions involving additions and disposals of fixed assets.

12. Recreation and Parks - Aquatics

Concessions at the aquatics center are managed by a third party, and an agreement is in place to provide a percentage of the proceeds to the City. The City has no knowledge of the total proceeds from concession sales and there is no control in place to verify that the payments received from the third party provider are accurate. A lack of verification provides an opportunity for the third party to withhold revenue owed to the City as agreed to by the contract. The City may not be collecting all revenue owed.

Recommendation: The following process enhancements are recommended in order to reduce the risk of uncollected revenue:

a. The best solution would be for the City to operate the Point of Sales system, collect the funds from the concession sales, and then distribute the amount due to the third party service provider.

b. If the above recommendation is not feasible, the City should obtain the daily or monthly Point of Sale system reports showing the total concession sales for the period to ensure that the payment received per the contract is accurate. In addition, the City should request and ensure that sales receipts are provided to the customer for each concession transaction to ensure that all sales transactions are recorded in the Point of Sale system.

Management Response: Several solutions under consideration for complying with this recommendation are as follows:

a. Require third party vendors to utilize the RecTrac system or a similar system that is capable of tracking sales.

b. Acquiring software that creates a profile for vending needs that allows the Recreation and Parks Department to track sales in real-time.

c. Require third-party vendors to forward detailed sales reports with sales receipts.

d. Run concessions in-house.

13. Recreation and Parks - Programs

Registration and collection of funds for most programs held by the City are conducted by third party service providers. These programs are managed by a third party and an agreement is in place to provide a percentage of the proceeds to the City. Typically, the City is unable to review registration lists. As a result, no control exists to verify that payments received from third party providers are accurate. A lack of registration verification provides opportunity for third party service providers to withhold revenue owed to the City as agreed to by contract. The City may not be collecting all the revenue owed.

Recommendation: Program registration and funds should be administered and collected by the City, and the proceeds due to the provider should be disbursed by the City based on the terms and conditions of the contractual agreements.

Management Response: This recommendation, along with a $65,000 budget increase to cover costs of implementing this change, has been proposed to the City Council for consideration in the upcoming budget cycle.

14. Recreation and Parks - Attendance

There is no method in place to adequately record the number of participants who utilize high traffic facilities, such as the aquatic centers or community/senior centers, so revenues may be matched.

Recommendations: The City may consider turnstiles or other means of recording attendance at the aquatics centers and other high traffic locations (e.g. community/senior centers, etc.) that record the number of participants that can be matched against gate revenues.

Management Response: The City will investigate turnstiles and other methods to account for the number of individuals using the pools, the Community Center and the Senior Center.

15. IT - Informal User Access Provisioning Process

Common formal procedures have not been established across the City to track and document requests and approvals for creating new user accounts (for employees and vendors), or for modifying user account permissions dependent upon a business need. Notable computer systems include Active Directory, RecTrac, and CMI, among others. A lack of a formal process for granting, approving, and documenting access for employees, including subcontractors, may lead to unauthorized users gaining access to sensitive information causing potential data leakage and data loss.

Recommendation: The City management should establish a formal user access provisioning process across the City that traces and maintains requests and approvals for creating new user accounts, and modifying user account permissions on computer systems.

Management Response: Response not yet received.

16. IT - Insufficient Independence in the User Access Provisioning Process

System owners are responsible for the approval and administration of user access to their respective applications without the requirement of a second approval from an independent resource. A lack of a process for independent validation of the design and operating effectiveness of internal controls may lead to the misrepresentation of internal controls, resulting in failed business processes and potential financial/reputational impact.

Recommendation: The City management should incorporate an independent resource, such as IT management, into the user access provisioning process. The independent resource should be required to review and provide a second approval for user requests to access business applications.

Management Response: Response not yet received.

17. IT - Informal User Access Deactivation Process

Common formal procedures have not been established across the City to timely track and document requests related to deactivations and closures of user accounts on computer systems. Failure to detect improper or stale access to computer systems increases the risk of unauthorized access to systems by external, as well as, internal threat actors.

Audit Note: Notable computer systems include Active Directory, RecTrac, CMI, as well as an emphasis on any web-based applications that may not require users to first authenticate via active directory prior to gaining system access from outside of the internal network.

Recommendation: The City management should establish a formal user access deactivation process across the organization that centrally tracks the completion of user account deactivations by IT staff and system owners upon documented notifications from HR or supervisors of employee separations.

Management Response: Response not yet received.

18. IT - Uncontrolled User Access

System owners (including Active Directory, RecTrac & Card Connect, and CMI) are not required to, nor do they perform, regular reviews of user accounts that can access critical information systems. The timely detection of inappropriate system access is limited without the periodic performance of this validation check. A lack of access-level reviews may lead to unauthorized access to data and the inability to identify and trace system activity, resulting in data loss.

Recommendation: The following process enhancements are recommended in order to reduce the risk of unauthorized access to computer systems and possible data loss:

a. The City management should update the Information Technology Security policy to include a requirement for system owners to conduct reviews of system access, including privileged system access, held by their respective system's user accounts for appropriateness at least twice annually. The scope of the reviews should not be limited to the following:

   i. Accounts with remote access to the network or email system.

   ii. Accounts with incompatible duties/access.

   iii. Dormant and disabled accounts.

   iv. Accounts with passwords that do not expire.

   v. Accounts with passwords unchanged according to policy.

b. The City of Hiliard management should require each system owner to perform and document the results of at least one user access review prior to the end of Q4 2018, in accordance with the updated Information Technology Security policy.

Management Response: Response not yet received.

19. IT - Unmanaged Privileged Access to RecTrac

With regards to how privileged system access to RecTrac is managed, the following was identified:

a. Privileged access to RecTrac is not limited to only employees with commensurate job duties.

b. Five Rec Supervisors hold local administrator access on both the transactional and web servers. Note: No more than two of the six supervisors use the privileged access to apply available upgrades/patches directly to RecTrac when responsible IT staff is unavailable.
c. Management does not take advantage of granular security features within the system capable of tightening current user access rights without compromising performance.

Unmanaged administrator access privileges may lead to unauthorized access to data.

Recommendation: The City management should implement more control over privileged access to the RecTrac system and server by considering the following:

a. Immediately review list of employees holding any privileged access to the RecTrac system and supporting servers. Remove access from any employees whose job duties are not compatible with the business needs for the privileged access.

b. Understand and apply applicable security features available within the RecTrac system to further restrict unnecessary access held by existing users as well as to the standard security profiles assigned to new users, as needed.

Management Response: Response not yet received.

20. IT - Untraceable Changes to RecTrac

Patches and other changes implemented directly to the RecTrac system servers by either IT staff or a Recreation and Parks supervisor are not required to be formally tracked and approved prior to their release to production. Changes that are ineffectively managed may lead to inappropriate changes being implemented or appropriate changes being mismanaged resulting in adverse impacts on the business or technology assets.

Recommendation: The following process enhancements are recommended in order to reduce the risk of inappropriate changes and/or updates to the RecTrac system and undesired affects on the organization or technical assets:

a. The City management should update the Information Technology Security policy requiring the business purpose, test results (if necessary) and proper approvals for all RecTrac updates and server security patches to be documented and retained prior to their releases into production.

b. New change management process should be enforced once the policy has been updated and approved.

c. IT - Insufficient Control Over Physical Datacenter Access

Management Response: Response not yet received.

21. IT - Insufficient Control Over Physical Data Center Access

Physical access to the primary datacenter in City Hall and the police department is managed in an informal manner that does not require all visitors to document and present legitimate business purposes to the IT Director for approval before their access is authorized and granted. Informal facilities/physical asset controls may lead to damage, loss of personnel safety, and loss of physical and information asset integrity due to various physical and environmental threats.

Recommendation: The following process enhancements are recommended in order to reduce the risk of damage or loss of physical data assets and/or personnel safety:

a. The City management should generate and review a report from the badge security system of all security badges assigned physical access to all datacenter facilities. Deactivate access that is stale or no longer required by the corresponding badge owner for relevant business purposes.

b. The City management should implement a formal process that tracks the employees, vendors and guests, their business purposes, and proper IT Director approvals for physical access requested to each data center. Particular consideration should be given to also document the expected timeframe for data center access granted to non-employees and expire the access accordingly.

Management Response: Response not yet received.

22. IT - Insufficient Information Technology Security Policy

The Information Technology Security policy was last revised over ten years ago in February 2008. Furthermore, the outdated policy does not define or enforce comprehensive requirements and standards for protecting the confidentiality, integrity and availability of the organization's information technology assets, such as:

a. IT Systems Security including password standards related to minimum password length and password history

b. Definitions of sensitive data and other key assets

c. Employee training and education requirements

d. Incident Management

e. Facilities Security

f. IT Security Roles and Responsibilities

g. Business Continuity and Disaster Recovery Plan

A lack of policies to appropriately manage user access to confidential data can result in data loss, data theft and potential reputational impact.

Employees may not be aware of their responsibilities related to information security leading to data breaches and service outages.

Recommendation: The following process enhancements are recommended in order to reduce the risk of data loss, data theft, and possible damage to organizational reputation:

a. The City management should update the Information Technology Security policy to define and enforce comprehensive requirements and the latest standards for protecting the confidentiality, integrity and availability of the organization's information technology assets. In addition to the considerations for the two aforementioned policy recommendations, the scope of the policy should not be limited to the following:

    i. IT Systems Security including password standards related to minimum password length and password history

    ii. Definitions of sensitive data and other key assets

    iii. Employee training and education requirements
    iv. Incident Management

v. Facilities Physical Security

vi. IT Security Roles and Responsibilities

vii. Business Continuity and Disaster Recovery Plan

b. The revised Information Technology Security policy should be reviewed and made effective immediately upon approval.

Management Response: Response not yet received.

23. IT - Lack of a Security Incident Response Plan

Plan, policy and procedures for responding to computer security incidents in an effective, efficient, and consistent manner have not been defined or implemented. A lack of incident response leads to businesses being reactive rather than proactive when data breaches and other issues occur.

Recommendation: The City management should develop and implement Computer Security Incident Response capabilities (plan, policy and procedures), in accordance with National Institute of Standards and Technology (NIST), including the following:

a. Security Incident Policy

b. Definition of computer security incidents

c. Roles and responsibilities of response team members

d. Triage procedures and escalation paths

e. Performance measures

f. Severity rating classification

g. Mitigation/remediation timelines

h. Reporting to external parties

Management Response: Response not yet received.

24. IT - Weak Password Controls

A number of RecTrac system password settings are not configured in alignment with leading practices to enforce adequate security over user access to the system. Notable insufficient password settings include the following:

a. Minimum password length = 0 characters

b. Password expiration set to 180 days which is not in accordance with the Information Technology Security policy of 90 days

c. Password complexity not enabled

d. Password history not enabled in accordance with the Information Technology Security Policy of 9 passwords remembered

e. Account lockout not enabled after determined number of invalid logon attempts

f. Password permitted to match username

Weak passwords can potentially allow malicious activity to result in unauthorized editing, disclosing, or deletion of sensitive data.

Recommendation: The City management should implement password settings in RecTrac that meet or exceed the following requirements:

a. minimum password length = 8 characters

b. maximum password age (expiration) = 90 days

c. complexity = enabled with upper & lower case, numbers, symbols

d. history enforced = 9 passwords remembered

e. account lockouts threshold = 9 invalid attempts

f. password match username = disable

Management Response: Response not yet received.

25. General - Knowledge Management Challenges

City of Hilliard is not acting to preserve the long-term success and competitiveness of the organization. There are limited tools in place to support the skills and knowledge retention with a number of departments. In particular, a succession plan has yet to be established to develop new leaders to fill key operations and management positions in the future. Furthermore, years of mission-critical information about existing technology systems and operational procedures have not been documented and shared between employees and key parts of the business.

Recommendation: the City management should consider the following:

a. Provide employees adequate opportunities for training and education to learn new skills and keep existing skills current.

b. Establish an internal document management process that provides centralized repository for storage and sharing of new and updated information to enable workflow progression.

V. Appendix A: Observations and Recommendations

The following is provided as a supplemental summary of the observations contained in this report and the risk ratings assigned to each observation. Ratings are defined at the base of the table.

Based on procedures performed, the following observation was noted. The table outlines the internal control rating assigned to the issue. The definition of each rating's significance is noted below the table.	**Internal Control Risk Rating**		
Observation	**1**	**2**	**3**
Clerk of Courts			
Observation 1: *Tickets and Fees*		X	
Observation 2: *Security of Confidential/Sensitive Information*		X	
Finance			
Observation 3: *Credit Card Usage*	X		
Observation 4: *Segregation of Duties*			X
Observation 5: *Accounting for Uncollected Revenue Earned*	X		
Observation 6: *Requisition and Purchase Orders*	X		
Observation 7: *Requisition and Purchase Orders*	X		
Human Resources			
Observation 8: *Payroll*		X	
Observation 9: *Mandatory Vacation*	X		
Observation 10: *Use of City Vehicles and Equipment*		X	
Land and Buildings			
Observation 11: *Fixed Asset Retirements and Additions*	X		
Recreation and Parks			
Observation 12: *Aquatics*		X	
Observation 13: *Programs*		X	
Observation 14: *Attendance*	X		
Information Technology			
Observation 15: *Informal User Access Provisioning Process*	X		
Observation 16: *Insufficient Independence in the User Access Provisioning Process*	X		
Observation 17: *Informal User Access Deactivation Process*		X	
Observation 18: *Uncontrolled User Access*	X		
Observation 19: *Unmanaged Privileged Access to RecTrac*	X		
Observation 20: *Untraceable Changes to RecTrac*			X
Observation 21: *Insufficient Control Over Physical Data Center Access*		X	
Observation 22: *Insufficient Information Technology Security Policy*		X	
Observation 23: *Lack of a Security Incident Response Plan*			X
Observation 24: *Weak Password Controls*		X	
General			
Observation 25: *Knowledge Management Challenges*	X		
Internal control risk ratings defined: 1 = High - unacceptable risk requiring immediate corrective action 2 = Moderate - undesirable risk requiring future corrective action 3 = Low - minor risk that management should assess for potential corrective action			