CITY OF HILLIARD

Business and Accounting Practices Review

September 7, 2018

SCHNEIDER DOWNS

Big Thinking. Personal Focus.

www.schneiderdowns.com

SCHNEIDER DOWNS

Big Thinking. Personal Focus.

September 7, 2018

Ms. Tracey 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 "City"). The accompanying report is to provide you with observations of the process, controls, and policies of the City.

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 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

Donald R. Owens
Shareholder
Risk Advisory Services

Table of Contents

I. Background

The City Hall of Hilliard, Ohio is located at 3800 Municipal Way, Hilliard, Ohio 43026. The City of Hilliard (the "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, it was requested that Schneider Downs recommend the consulting services that should be performed to verify appropriate controls are in place to effectively safeguard the City's funds and assets.

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

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

III. Approach

Schneider Downs & Co., Inc. (Schneider Downs) was engaged to perform a review of the City of Hilliard, 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 in scope were defined, Schneider Downs met with the City's management and key personnel within each of the following groups (function/position):

- Mayor/Commissions;
- Mayor/City Clerk;
- Mayor/Clerk of Courts;
- Department of Economic Development/Economic Development Director;
- Department of Law/Law Director;

- Department of Communications & IT/Communications Director;
- Division of Building/Service Director;
- Division of Engineering/Service Director;
- Division of Service/Service Director;
- Lands and Building/Lands and Building Director;
- Division of Parks and Recreation/Recreation and Parks Director;
- Department of Finance/Finance Director;
- Department of Tax/Deputy Finance Director;
- Human Resources/Human Resources Director; and
- 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 Rec 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) on, at least, a monthly basis to evaluate the propriety of adjustments and assess trends.

2. Clerk of Courts - Physical Access

Physical access to the Clerk of Court room is not secure. The door to the Clerk of Courts office does not have a lock to prevent inappropriate or unauthorized access to confidential records. Unauthorized physical access could lead to exposure or theft of sensitive personal data.

Recommendations: The following process enhancements are recommended in order to reduce the risk of theft of or inappropriate access to confidential records.

a. A security lock should be installed on the Clerk of Courts office door sufficient to prevent unauthorized access outside normal business hours or when unattended by the Clerk of Courts.

b. Recommend Key FOBs for any offices or rooms containing cash, valuables, and confidential information.

3. Finance - Credit Card Usage

There is no formal accountability for City of Hilliard credit card transactions or ability to trace back to the individuals using the card. Currently, there are two credit cards in use: one for the Finance Department, which is also used by IT & Communications, and one for the Police Department. The card numbers can be used by any individual with knowledge of the credit card number or 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, recommend that the City of Hilliard credit cards be assigned on an individual basis rather than a department basis.

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 could 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, is it recommended that the Finance Department, as an independent function, review 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.

5. Finance - Accounting for Uncollected Revenue Earned

Revenue due the City of Hilliard 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, which could 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 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.

6. Finance - Requisition and Purchase Orders

All Finance Department personnel have access rights 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.

7. Human Resources - Payroll

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

Policy does not allow the Payroll Specialist to approve time and move to CMI if an employee's time is not approved, but the application security with the Right Stuff does not prevent the Payroll Specialist from moving unapproved time from Right Stuff to CMI. A lack of application control configuration setting can lead to inappropriate transfer of unapproved time.

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 could result in inappropriate payroll activity that is not detected. A lack of independent review can result in undetected 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 Detailed Work Register shows the full payroll rather than just the changes that were input 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.

b. If possible, revise the configuration settings to prevent the payroll specialist (or other assigned users) from transferring unapproved employee hours to the CMI payroll system.

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

d. 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.

8. Land and Buildings - Fixed Asset Retirements and Additions

When fixed assets are removed or replaced with new assets by the Land and Buildings Department, there is no formal control or process being performed to identify and communicate the asset retirements and asset additions to the Finance Department to update the Fixed Asset Register. A lack of oversight and communication between Land and Buildings and Finance Departments may cause inaccurate reporting on the Fixed Asset Register and noncompliance with accounting standards.

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 accurate and complete updates are made to the Fixed Asset Register and revisions are appropriately made to the asset net book values.

9. 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 of Hilliard. As the City has no visibility to the total concession sales, there is no control in place to verify 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 of Hilliard as agreed to by contract. The City of Hilliard 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 of Hilliard 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 of Hilliard 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 of Hilliard 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.

10. Recreation and Parks - Programs

Registration and collection of funds for most programs held by the City of Hilliard 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 of Hilliard 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 of Hilliard as agreed to by contract. The City may not be collecting all the revenue owed.

Recommendation: Programs 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 per the contractual agreements.

11. IT - Informal User Access Provisioning Process

Common formal procedures have not been established across the organization 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 and including subcontractors, may lead to unauthorized users gaining access to sensitive information causing potential data leakage and data loss.

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

12. 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 second approval from an independent resource. A lack of a process for independent validation of the design and operating effectiveness of internal controls can lead to the misrepresentation of internal controls, resulting in failed business processes and potential financial / reputational impact.

Recommendation: The City of Hilliard 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's requests to access business applications.

13. IT - Informal User Access Deactivation Process

Common formal procedures have not been established across the organization to track and document requests related to deactivations and closures of user accounts on computer systems in a timely manner. 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 of Hilliard 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.

14. 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 of Hilliard 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.

15. IT - Unmanaged Privileged Access to RecTrac

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

- Privileged access to RecTrac is not limited to only employees with commensurate job duties.
- 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.
- 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 of Hilliard 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.

16. 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 of Hilliard 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

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

18. IT - Insufficient Information Technology Security Policy

The Information Technology Security policy was last revised over ten years ago in February of 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:

- IT Systems Security including password standards related to minimum password length and password history
- Definitions of sensitive data and other key assets
- Employee training and education requirements
- Incident Management
- Facilities Security
- IT Security Roles and Responsibilities
- 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 of Hilliard 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.

19. 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 of Hilliard 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

20. 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:

- Minimum password length = 0 characters
- Password expiration set to 180 days which is not in accordance with the Information Technology Security policy of 90 days
- Password complexity not enabled
- Password history not enabled in accordance with the Information Technology Security Policy of 9 passwords remembered
- Account lockout not enabled after determined number of invalid logon attempts
- 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 of Hilliard 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 w/upper & lower case, numbers, symbols

d. history enforced = 9 passwords remembered

e. account lockouts threshold = 9 invalid attempts

f. password match username = disable

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: *Physical Access*		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
Human Resources			
Observation 7: *Payroll*		X	
Land and Buildings			
Observation 8: *Fixed Asset Retirements and Additions*	X		
Recreation and Parks			
Observation 9: *Aquatics*		X	
Observation 10: *Programs*		X	
Information Technology			
Observation 11: *Informal User Access Provisioning Process*	X		
Observation 12: *Insufficient Independence in the User Access Provisioning Process*	X		
Observation 13: *Informal User Access Deactivation Process*		X	
Observation 14: *Uncontrolled User Access*	X		
Observation 15: *Unmanaged Privileged Access to RecTrac*	X		
Observation 16: *Untraceable Changes to RecTrac*			X
Observation 17: *Insufficient Control Over Physical Data Center Access*		X	
Observation 18: *Insufficient Information Technology Security Policy*		X	
Observation 19: *Lack of a Security Incident Response Plan*			X
Observation 20: *Weak Password Controls*		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			