Internal Audit Report 16-02
Information Technology Audit
June 2016

City of Sioux Falls

Providing a Better Quality of Life for You!

City of Sioux Falls
Internal Audit Department
Carnegie Town Hall
235 W. 10th Street
Sioux Falls, SD 57117-7402
www.siouxfalls.org/council/internal-audit

INFFORMATION TECHNOLOGY AUDIT
INTERNAL AUDIT REPORT 16-02

INTRODUCTION

Information Technology (IT) is a division of the Central Services major organizational unit. The division develops, implements, and maintains computer systems in support of the City's internal and external operations.

BACKGROUND

The IT department oversees the City's Information Technology program which includes all computer operations, technical support, systems analysis, programming, database management, security management, and IT training. They provide a wide range of technology services and resources to ensure employees are supplied with the necessary tools that enable them to deliver quality services to their customers. IT is responsible for supporting approximately 1,650 users and numerous computer applications including Munis (Finance), RecTrac (Parks and Recreation), EnerGov (Planning and Building), CIS Infinity (Utility Billing), and Paradigm (Landfill). They are the City's resource for advisement and direction on technology services and for establishing technology best practices, standardization, and guidance. During 2015, the IT division was authorized 27 full-time employees and had an operating budget of $3.7 million.

IT also manages the Technology Revolving Fund. This internal service fund was set-up for the purpose of tracking technology related expenses for all City departments, to ensure technology related purchases meet the business objectives set forth by each department, and to aid in simplifying the technology budget process.

OBJECTIVES

The objectives of this audit were to:

1. Determine if general controls are in place and functioning.
2. Determine if application controls for Munis are in place and functioning.
3. Determine if the City is using leading practices for IT hardware inventory management.

SCOPE AND METHODOLOGY

The scope of this audit focused on the review of IT general controls, application controls for Munis, and IT hardware inventory management practices as they currently exist or as they occurred in 2015. General controls are controls over the operation and management of all computer processing activities. They are also known as infrastructure controls.

Application controls are controls over individual business processes or application systems. Therefore, they are specific to each individual application, whereas general controls are not. Since the IT department supports numerous applications, our audit focused on the City's main financial software system, Munis. Our audit work included the following:

- Review of written policies and procedures, Executive Orders, 2015 IT Budget, and IT organizational chart.
- Review of prior audit recommendations.
- Review of prior audit report and other local government audit reports.
- Interviews with IT and Finance management and department staff.
- Observation of data center and offsite backup location.
- Testing of new IT employee hires for a criminal background investigation prior to employment with the City.
- Testing of a randomly selected sample of terminated employees for removal of network access.
- Review of active roles and users within the Munis system.
- Review a sample of purchase orders to determine they are processed accurately, completely, and timely within the Munis application software.
- Perform an analytical review of manual, non-recurring journal entries to determine they are processed accurately, completely, and timely within the Munis application software.
- Testing of a sample of hardware inventory items from the IT Inventory database for one randomly selected location to determine the accuracy of the database.

RESULTS

IT GENERAL CONTROLS

Physical Security

We observed the physical access and environmental controls in place. We determined that a criminal background check is performed on each new hire within the IT department prior to employment with the City. Physical access to the data center and server room is controlled by an electronic card swipe system, restricted to IT and Facilities Maintenance staff, and monitored by four surveillance cameras. Non-IT staff needing access to the department, data center, or server room must be escorted by an IT staff member and a log is kept of all guests who access the server room.

Access controls, such as firewalls, usernames and passwords, and user roles are in place to protect data from unauthorized modification, loss, and disclosure. Department managers must submit a request to the IT department in order for a user to be created or modified. User access (for example, read, modify, delete) is restricted based on department, job title, and job function. Network access for terminated employees is removed within twenty-four hours of their last working day. A password policy is in place over network accounts which outline the minimum number and type of characters that must be used when creating a password and how often they need to be changed. However, in order to increase the overall security position of the City, the password policy restrictions should be redefined. See recommendation 1 below.

We determined that adequate environmental controls are in place including fire detection and suppression equipment, redundant air conditioning units, raised floors, and uninterruptible and emergency power supply units. Regular maintenance and inspection is performed to ensure the equipment is working properly. The server room is clean and free of combustible materials and the room temperature is continually monitored.

Backup and Contingency Planning

We verified the IT department has a written Continuity of Operations Plan to serve as a tool to help the City's departments effectively resume technology operations and day-to-day core services in the event that a natural disaster or an unplanned interruption occurs. The department maintains a secondary backup location of all vital systems, applications, and equipment. Critical files and operations are backed up to this location and can be restored if needed. This location is protected from damages that could occur from extreme temperatures, water, fire, and forced entry. The City also rents an alternate storage and processing site that can be used in emergency situations. Annual exercises and regular meetings are held to keep IT staff informed of the procedures to follow in the event of a disaster.

Change Management

We determined a change management policy has been drafted and is currently being followed. However, the policy, which is a part of the Information Security Program Plan, has not been finalized and approved by appropriate personnel. See recommendation 2 below. When required changes are needed to information system resources (for example, software programs and hardware configurations), a proposal is submitted to and reviewed by the IT department. Upon approval by the IT department, changes are tested, validated, and documented prior to implementation within the operating system. Certain changes must also go through various levels of authorization by IT management prior to implementation.

Through discussion with IT management and review of procedures, we determined vulnerability scans are performed monthly to identify areas that could be exploited within the information system. Significant vulnerabilities identified are remediated within a month. The department has also established effective programs for patch management, virus protection, and other emerging threats such as phishing, malware, and ransomware to aid in protecting computer systems from attack.

Information Security Management

The department has drafted an Information Security Program Plan (see recommendation 2 below) which defines the roles and responsibilities of IT management, IT staff, and City employees in ensuring information and information systems that support the operations and assets of the City are secure. The department performs periodic risk assessments to identify reasonable threats to the system, to determine the likelihood and impact of the threats, and whether policies, procedures, or controls are in place to mitigate the risks. User security awareness is maintained through training, distribution of policies and procedures, and annual performance reviews.

IT management understands the importance of information security and, therefore, had an external IT consultant perform an independent security review during February 2016. The purpose of the review was to determine that adequate network and security controls exist and are working as intended. We discussed the results of the review with management and determined that management has appropriately addressed each item. The overall impact of this review has resulted in strengthening the City’s security infrastructure.

APPLICATION CONTROLS - MUNIS

We determined that access to Munis is restricted through the use of user roles. User accounts are assigned to a role(s) in Munis based on their job description and responsibilities. Therefore, users only have access to the data or transactions that are required for them to perform their job function. We reviewed the active roles and assigned users for the critical financial activities and verified they are appropriate. We noted that select employees in the Finance and IT department have access to assign user roles within Munis. However, based on our discussion with Finance personnel, the access is not approved by anyone or reviewed regularly. See recommendation 3 below.

We selected a sample of purchase orders and determined that the source documents were processed accurately, completely, and timely by the application software and an audit trail exists for who initiated and approved the transaction. We also performed an analytical review of manual, non-recurring journal entries and determined adequate support and segregation of duties exists. We concluded that applications controls are working properly within Munis.

IT HARDWARE INVENTORY MANAGEMENT

The IT department manages and tracks IT hardware inventory items such as servers, laptops, desktops, tablets, monitors, printers, etc. in a database called IT Inventory. We determined inventory items are assigned a unique identifier upon receipt, tagged, and recorded in the database. The item is then tracked throughout its lifecycle including deployment and disposal. We verified hardware inventory is properly surplused and/or disposed of when it is no longer used, no longer works, or is at the end of its lifecycle.

Through discussion with management, we determined the hard drives of desktops, laptops, servers, etc. are removed, properly wiped of all data, and are not recycled for reuse.

We reviewed a sample of hardware inventory items from the IT Inventory database. We traced the sample items to physical presence and verified the inventory information (asset tag, user, serial number, location, department) shown in the listing was correct. We also reviewed the premises to determine if there were additional IT hardware items in this location that were not shown on the listing. Of the 28 items selected for testing, we noted 3 instances where the information in the database was inaccurate or items were missing from the database. See recommendation 4 below.

RECOMMENDATIONS

We made the following recommendations that address the above referenced results.

1) Both the user and system administrator password policy requirements should be redefined to increase the security position of the City. Password security best practices suggest that long passwords, minimum of ten characters, or the use of passphrases dramatically improve security.

   Management's Response: The current password policy requires the use of 3 of 4 of the following: lower case, upper case, numeric, special character. We periodically educate the employees on the best practices of choosing strong passwords such as the use of passphrases. We continue to improve our password strength requirements; however, we are also bound by the limitations of some vendor applications. We are in the process of an extensive review of these vendor requirements and will push for a ten character minimum password by the end of Q1 2017.

   Management Representative Responding: Jon Klemme, IT Manager

   Date of expected implementation: March 31, 2017

2) IT department policies and procedures should be regularly reviewed and updated, approved by management, and communicated to applicable staff. Written policies and procedures are critical to the overall internal control system as they define employee responsibilities and establish accountability and consistency.

   Management's Response: We feel strongly that this guiding security policy allows us to increase our security posture through the use of the latest industry standard security principles, educating our end users, and communicating expectations to all departments. The final approval of this policy will be achieved by August 1, 2016.

Management Representative Responding: Jon Klemme, IT Manager

Date of expected implementation: August 1, 2016

3) Finance management should develop a written policy in regards to who grants and approves access to the various user roles in Munis. The policy should also include how often the active user roles are reviewed and who is responsible for reviewing them.

   Management's Response: Finance has discussed a software enhancement with Munis that would allow for the establishment of an approval process for access to the user role functionality within the software. Recognizing that a software enhancement may not be available in the immediate future, Finance and IT have instituted a regular review of user roles by appropriate managers and will develop a written policy for who should have access to this functionality and how often roles will be reviewed.

   Management Representative Responding: Tom Huber, Assistant Director of Finance

   Date of expected implementation: October 1, 2016

4) IT management should develop a process to periodically confirm the accuracy of the IT Inventory database.

   Management's Response: The Information Technology group has reviewed our inventory practices with the Finance Department to improve our information tracking on the technology assets. We have added new software tools to scan the network to gather information about these assets. These tools will be used to reconcile the equipment that is deployed. We will conduct these reviews on a semi-annual basis.

   Management Representative Responding: Jon Klemme, IT Manager

   Date of expected implementation: October 1, 2016

CONCLUSION

We conclude that IT general controls, application controls for Munis, and IT hardware inventory management practices are appropriate and functioning properly. The implementation of the above recommendations will strengthen controls further. IT management is very knowledgeable about various risks associated with information technology and has been proactive in addressing these risks and in using industry best practices to achieve greater efficiencies. We would like to thank the IT and Finance employees for their cooperation and courtesy shown to us during the course of the audit.

AUTHORIZATION

The Sioux Falls City Council approved this audit by resolution in December 2014 as part of the 2015 Annual Audit Program. The Internal Audit division operates under the authority of an Internal Audit Charter adopted by City Council resolution 11-13.

AUDIT STANDARDS

This audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* issued by the Institute of Internal Auditors.

STATEMENT OF INDEPENDENCE

Internal Audit is administratively and operationally independent of the programs and departments it audits, both in appearance and in fact. The Internal Audit Manager is accountable to an Audit Committee appointed by the City Council per section 32.022 of the Code of Ordinances of Sioux Falls, SD.

DISTRIBUTION OF REPORT

This report is intended for the information and use of the Mayor and City Council, management, and others within the City of Sioux Falls. However, the report is a matter of public record and its distribution is not limited.

PERFORMED BY

Ashley Stroschein
Internal Auditor