INFORMATION TECHNOLOGY GENERAL CONTROLS

April 2016

RubinBrown LLP
Certified Public Accountants & Business Consultants

One North Brentwood
Saint Louis, MO 63105

T 314.290.3300
F 314.290.3400

W rubinbrown.com
E info@rubinbrown.com

July 29, 2016

Finance and Administration Committee
City of Springfield
840 Boonville Ave.
Springfield, Missouri 65802

Re: IT General Controls Internal Audit

Dear Committee Members:

In conjunction with our overall engagement to provide internal audit services to the City of Springfield, we have completed our internal audit of the City's Information Technology General Controls (ITGCs). Our services were performed in accordance with the International Standards for the Professional Practice of Internal Auditing, as promulgated by the Institute of Internal Auditors (IIA).

The accompanying report includes an Executive Summary, Observations and Recommendations and Process Improvement Opportunities. Because the procedures performed in conjunction with the review are more limited than would be necessary to provide an opinion on the system of internal accounting controls taken as a whole, such an opinion is not expressed. In addition, the engagement did not include a detailed audit of transactions that would be required to discover fraud, defalcations or other irregularities.

This report is intended solely for the information and use of management and the City Council and is not intended to be, and should not be, used by anyone other than the specified parties. City of Springfield external auditors may be provided with a copy of this report in connection with fulfilling their responsibilities.

We would like to express our gratitude to all employees involved with this project. Each person involved was accessible and responsive to our requests for information.

Sincerely,

RUBINBROWN LLP

Richard R. Feldt, CPA
Partner
Direct Dial Number: 314.290.3220
E-mail: rick.feldt@rubinbrown.com

Christina Solomon, CPA
Partner
Direct Dial Number: 314.290.3497
E-mail: chistina.solomon@rubinbrown.com

Enclosures
cc: David Holtmann
Mary Mannix-Decker
Jeff Coiner

an independent member of BAKER TILLY INTERNATIONAL

CITY OF SPRINGFIELD
IT GENERAL CONTROLS INTERNAL AUDIT

Table of Contents

CITY OF SPRINGFIELD
IT General Controls Internal Audit
Executive Summary

Project Overview and Scope

We completed our review of the City of Springfield's IT General Controls. The objectives of our review were to:

- Identify existing policies and practices related to Information Technology General Controls (ITGC).
- Evaluate compliance with existing ITGC policies.
- Develop recommendations to improve the efficiency of IT processes, and adherence to industry best practices.

Our review included transactions from January 1, 2015 through December 31, 2015. We completed the following procedures:

- Performed in-person interviews with Information Systems (IS) personnel. The objective of the interviews will be to gain an understanding of and document the following processes:
    - IT governance;
    - Logical access;
    - Change management;
    - Backup and recovery;
    - Physical access / Security to IT assets.

- We performed the following limited testing of transactions to verify the documented processes were operating as intended:
    - User account additions and terminations were properly approved and changes were made in Oracle;
    - User access reviews were approved and changes were completed in Oracle;
    - Patches to Oracle were approved and tested prior to deployment into production;
    - Physical access to the data centers and badge access software is properly controlled;
    - Backup failures for the network file servers and Oracle system are successfully rerun within 24 hours;
    - Service tickets submitted to the help desk are resolved timely and proper approvals are obtained, if necessary; and
    - Administrator accounts for the Oracle system are properly controlled.
- Evaluated trends using data analysis for the areas identified above; and
- Compared current practices to industry best practices, including an evaluation of current capabilities, to achieve an effective and efficient control environment.

CITY OF SPRINGFIELD
IT General Controls Internal Audit
Executive Summary

Background

The IS department consists of five 5 functional areas: enterprise systems and city software, telecomm (phones), help desk, geographical information systems (GIS), and network. The department provides a communications network capable of supporting the city's mission. A network of "WiFi" wireless connection for citizen use within select city facilities is also maintained. The department manages the acquisitions of hardware and software by city departments through research assistance, team participation, and leadership during implementation. IS maintains the information technology resources once they are acquired. An internal support help desk takes calls, logs problems, and provides solution to any employee that is utilizing electronic equipment, including desktop and laptop computers, fax machines, network services, and telephones. The department also provides support for the city's internet and intranet, and internal website, as well as many other civic organizations sites.

Best Practices

Based on our review, the following internal controls are in place and, in our opinion, represent a best practice:

- The City has as Administrative Memo (#37) that provides policy for multiple IS areas including hardware and software acquisitions, software development, employee additions/terminations, mobile device controls, and passwords.
- The CityShare process to add and terminate Oracle users through the help desk is in place and operating effectively;
- The 2015 user access review for Oracle was well executed, responded to timely, and changes were made within the system in a timely manner; and
- For the limited sample of help desk tickets we reviewed, the average days to close a service request was 8 days and if approvals were necessary, they were obtained.

Observations and Recommendations

We determined that IT General Controls are adequate; however, our risk review noted the following procedures that we would consider internal control weaknesses:

- There is no City-wide training for cyber security. The city has experienced four cybersecurity incidents during the last six months.
- Network equipment is not barcoded or periodically inventoried.
- Changes made to the Oracle source code are not logged.

All observations and recommendations were discussed with management. Details are noted in the schedules attached immediately hereafter.

City of Springfield
IT General Controls Internal Audit
Observations & Recommendations

	Process/Procedure	Observation and Risk	Recommendation	Management Response
1	Employees complete Information Systems training when hired.	Observation: Cybersecurity training and annual or biennial training is not required to be completed. In the past six months, four ransomware incidents have occurred primarily because City users have inadvertently downloaded unauthorized software and introduced it into the City's network. Risk: Continued cybersecurity incidents, which could expose the City's information to unauthorized users.	Require initial cybersecurity training for all City employees that access the network. Implement a training requirement of every other year for cybersecurity.	**IS Director** We have created a Cyber Security Awareness Committee from within IS and we agree with the need for employee training. We have identified options for online training and plan to proceed with a training program for all employees by **December 15, 2016.**
2	A list of network equipment is maintained by the IS department.	Observation: The listing of network equipment does not include a property tag number because the equipment is not part of the City's property book. Additionally, it was unclear that network asset inventories were regularly performed. Risk: Loss of control over network assets.	Barcode network equipment and input it into the City's property system. Perform annual network asset inventories using software tools and the physical asset listing. Ensure that the electronic listing matches the physical listing.	**Network Manager** We have ordered inventory labels for our network equipment and we will complete a physical inventory of our network equipment by **October 1, 2016.** We will also review the inventory list annually.

	Process/Procedure	Observation and Risk	Recommendation	Management Response
3	City employees must use a badge to access data centers located at the Busch building and an underground facility. Access to the badge software was properly controlled.	Observation: We reviewed a listing of 72 badges with access to the data centers. The badges for fifty-five individuals had the following issues: possibly terminated, access does not appear necessary, has two badges. Risk: Unauthorized access to the Busch building data center.	Disable unnecessary access to the data center and other physical IS locations. Perform a review of data center access every other year.	**Network Manager** Unnecessary access to the data center and other physical IS locations has been removed as of **May 1, 2016.** Access to the data center will be reviewed annually.
4	Systems Administrators and Administrative Systems Analysts have access to develop code and migrate it into the production environment for the Oracle system.	Observation: Changes made to the source code of Oracle are not logged. Risk: Unauthorized changes could be made to the Financial and HR system without the knowledge of Information Systems management.	Log changes made to Oracle and retain the logs for a management defined period, but at least a year.	**Sr. Database Administrator** We will enable logging of changes and keep them for 1 year. This will have an impact on hard drive storage and performance on the Oracle system and may require additional funding to address those issues. **Target Date: July 1, 2016**

	Process/Procedure	Observation and Risk	Recommendation	Management Response
5	Network file servers are backed up on a daily basis. A log can be produced which shows whether the backup has been successful within the last 30 days.	Observation: Logs which show whether the network file server backup is successful or if it failed are only kept for 30 days. Risk: Inability to identify a volume or server that is continuously failing and to investigate the root cause of that failure.	Keep logs of the network file servers for a management defined period, but at least a year.	**Network Manager** We have updated the log file retention period to 365 days. This may impact backup performance and system availability. We will monitor the impact and review annually to be sure we are meeting our business requirements. **Target Date: May 4, 2016**

	Process/Procedure	Observation and Risk	Recommendation	Management Response
6	Patches to the Oracle financial system must be properly approved and tested prior to deployment to production. Users must also be notified of downtime if patch deployment will affect server uptime.	Observation: • For ten (10) of ten (10) patches, users were properly notified of downtime prior to deployment. • For eight (8) of ten (10) patches, evidence was available which showed the patch was approved or tested prior to deployment into the production environment. o For one patch, evidence was not available to show the patch had been tested prior to deployment. o For one patch, evidence was not available to show the patch was approved and tested prior to production. Risk: Unauthorized changes to the production environment that could cause unplanned downtime.	Ensure that patches are properly authorized, and that documentation of testing is documented.	**IS Director** Management believes the current process is adequate and that patches are properly authorized and tested. All patches are documented and tracked. All changes are communicated with the Finance and HR representatives on the Citylink Support Team. There are some critical security patch exceptions that must be applied as an emergency update that may not allow for normal functional testing to be completed. We understand the risks & benefits and will weigh them on a case-by-case basis if this type of exception arises. **Target Date: May 1, 2016**

	Process/Procedure	Observation and Risk	Recommendation	Management Response
7	Administrator accounts are used to make changes to the Oracle Financial and Human Resources system. We obtained a listing of administrator accounts and noted there were eleven (11) accounts.	Observation: Two (2) of eleven (11) administrator accounts were active but unused. The default password on these two accounts had not been changed since implementation. Risk: Unauthorized changes to the Financial system.	Disable unused administrator accounts for the Financial and HR system, and any other enterprise wide systems.	**Sr. Administrative System Analyst** The unused administrator accounts have been disabled. Administrator accounts will be reviewed annually during the end-user audit. Unused accounts that are found will be disabled immediately. **Target Date: May 1, 2016**

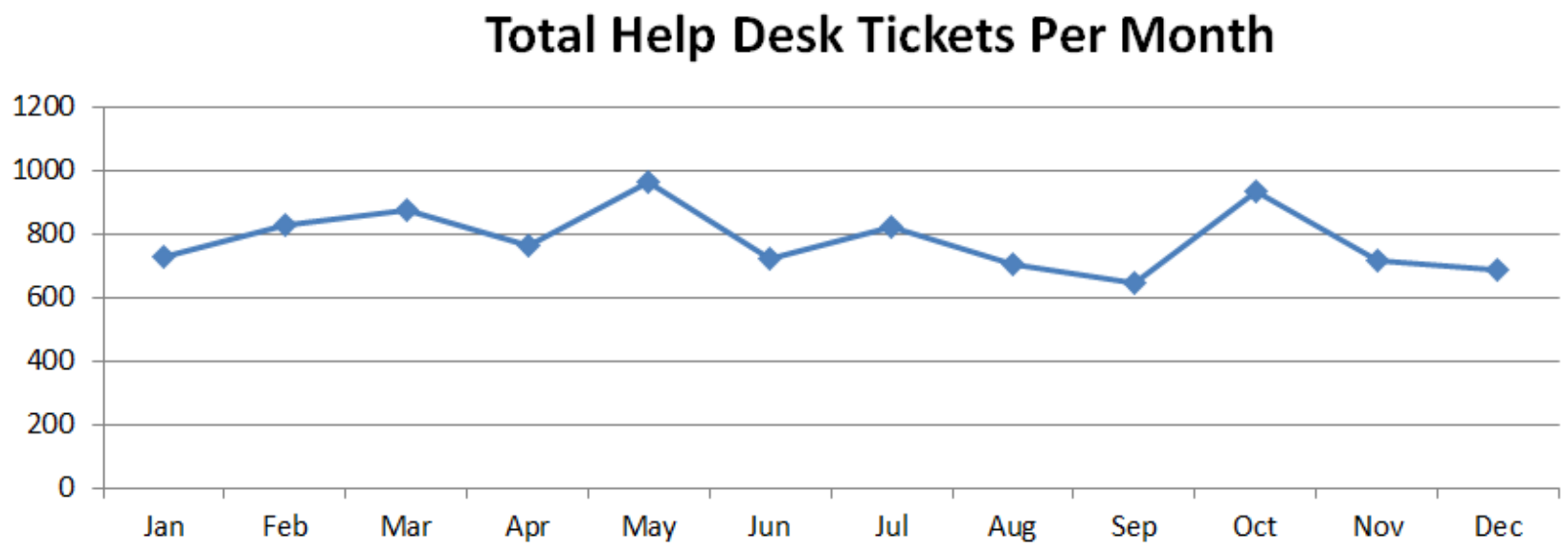
City of Springfield
IT General Controls Internal Audit
Process Improvement Opportunities

We noted the following process improvements during our review. These observations are not considered an internal controls weakness; however, we do recommend management consider each observation and take action where appropriate.

	Observation	Process Improvement	Management Response
1	The City's Emergency Response plan for IS security incidents has not been updated since 2010. It is 25 pages long.	Update the security incident response plan and consider making it more targeted. A shorter and more concise document will be more user friendly for the first responders.	**IS Director** Agreed. The IS Leadership Team will review and update the plan and make it more concise. **March 31, 2017**
2	The City maintains a listing of 329 information systems software on an Excel spreadsheet. The sheet contains a description of the software, the developer responsible for maintaining the software, and the complexity of the program.	Utilize versioning software to store each iteration of the program code, including the most recent source code. Versioning software can also be used to store developers' notes, version information and the other information that is currently stored in Excel.	**IS Director** I.S. will review options and consider this for our FY2018 budget requests. **March 31, 2017**
3	A systems administrator for the Police Records database is functionally assigned to the Police Department. Two Network Administrators are functionally assigned to the Airport. Additionally, there are individuals assigned to the 911 emergency communications department, traffic department, and municipal court departments that perform primarily IS job functions.	Consider functionally organizing individuals with primarily IS responsibilities under the IS department.	**IS Director** Management agrees and is supportive of a centralized I.S. organization for all of the City's technologies. The need for network and computer system security and the implementation of IT services, whether on premises or cloud-based, requires tightly integrated and coordinated effort City-wide. This need is best met with a centralized staff with dedicated support for critical services. **TBD**

Help Desk Tickets

Below are metrics related to an analysis of 2015 Help Desk ticket volume and categories. This information is provided for management's use.



Help desk tickets by Category for 2015