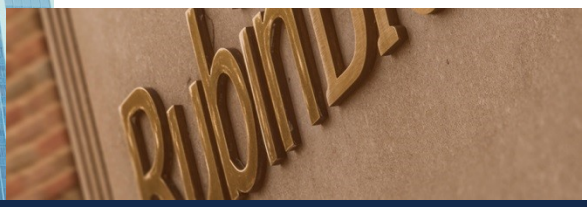

City of Springfield, Missouri

Information Technology General Controls
Internal Audit

Fieldwork August 2019

CERTIFIED PUBLIC ACCOUNTANTS & BUSINESS CONSULTANTS

RubinBrown

One North Brentwood
Suite 1100
St. Louis, MO 63105

T: 314.290.3300
E: info@rubinbrown.com
www.RubinBrown.com

CERTIFIED PUBLIC ACCOUNTANTS & BUSINESS CONSULTANTS

April 8, 2020

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

Re: Information Technology General Controls (ITGC) Internal Audit

Dear Committee Members:

In conjunction with our overall engagement to provide internal audit services to City of Springfield ("City"), we have completed our assessment of the City's ITGC controls for the Information Systems department. 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, our Observations and Recommendations and an Appendix. Because the procedures performed in conjunction with the internal audit 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. In addition, we understand that the City may be required to make our report, once finalized, available under sunshine laws.

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

Christina Solomon

Christina Solomon, CPA/CFF, CFE, CGMA
Partner
Direct Dial Number: 314.290.3497
E-mail: christina.solomon@rubinbrown.com

cc: Matt Roberts Jody Vernon
Pam Cummings David Holtmann

Table of Contents

Executive Summary

Project Overview and Scope

The objectives of the information technology general controls (ITGC) internal audit for City were to:

1. Identify existing policies and practices related to IT general controls, and determine that there are controls in place for IT processes, and that they are operating effectively.

2. Evaluate current IT business processes for efficiencies and applicability of best practices.

Our internal audit included activity from July 1, 2018 through the end of August, 2019. In order to achieve the objectives above, we performed the following activities:

- Performed in-person interviews with Information Systems (IS) personnel, and personnel from departments with data center/server rooms and switch closets, including Public Works (Traffic), Environmental Services, Emergency Communications, Workforce Development, and Parks. The objectives of the interviews were to gain an understanding of and document the following processes. This information was used to create a narrative of the current ITGC management processes and related policies:
    - IT governance;
    - Logical access;
    - Change management;
    - Patch management;
    - Backup and recovery;
    - Physical access/security to IT assets.

- We performed the following limited testing to verify the documented processes were operating as intended:
    - Logical Access/Password Configurations - We compared application and operating system password configurations to best practices.
    - We evaluated the patch management process and change management process to verify that patches were approved and tested prior to implementation into production, and that the Help Desk Break-Fixes are resolved in a timely manner.
    - We evaluated badge access for the City's main data center, Emergency Communications, and Environmental Services' SCADA office.
    - We evaluated backups for Oracle and the network to determine whether a process was in place to identify and follow up on failures.

Background

The Information Systems (IS) department consists of approximately 34 employees within four different areas:

- Network
- Help Desk
- Geographical Information Systems (GIS)
- Enterprise Systems and City Software

The annual budget is approximately $4 million. The Information Systems department provides the following services: a communications network, new acquisitions of hardware and software, maintenance of the City Information Technology resources and investments, an internal support help desk, support for the City's internet and intranet / internal websites, and back-up power generators to provide 3 days of energy in case of City-wide failure.

In addition to the IS department, other departments have IS analysts and administrators that are functionally organized within the department. Below is an overview of departments and systems within the scope of our internal audit.

Department	Related Systems
Information Systems	Network, CityLink (Oracle ERP and database), ManageEngine/Desktop Central (Help desk software)
Public Works (Traffic)	Network, TransSuite
Environmental Services	SCADA, Ladder Logic tool within SCADA, LIMS and MXView
Emergency Communications	Network, Computer Aided Dispatch (CAD), 911 Telephone system, Radio system, Logging Recorder, Paging, and Fire department alerting system.
Workforce Development	Uses the systems provided by IS, as well as IS support
Parks	Active (the point-of-sale system for customer transactions)

Best practices

Based on discussions with management personnel, the following processes are in place at the City and represent best practices:

- Help desk break-fix requests are resolved in a timely manner. Additionally, the IS department has the ability to produce reporting on requests using ManageEngine.
- The City has as Administrative Memo (#37) that provides policy for multiple IS areas including hardware and software acquisitions, software development, employee additions/terminations, and mobile device controls.

Observations and Recommendations

Observations from our internal audit are noted below:

- The COOP plan was last updated in 2016 and testing of the plan has not occurred on an annual basis.
- Periodic user access reviews are being performed, but not documented.
- The Senior Database Administrator has system administrator access to the application, and also has the ability to install, design, migrate data, and configure data within the Oracle database (as a database administrator).
- A formal written password policy was not in effect for the City. The Oracle database was not configured to enforce password parameters. Minimum password age for SCADA was "0". Password history (passwords that cannot be reused) was, zero for the SCADA system at Environmental Services, five for Public Works (Traffic) network, and five for Active, the Parks application.
- We reviewed a sample of 10 computer patches and found that four patches were not fully deployed and followed up on in a timely manner.
- We reviewed physical access controls to data rooms and data closets across the City and found that access was not properly restricted at the main data room, the SCADA data closet, the Workforce Development data room, and the Parks department switch rooms.
- Patches for the Public Works (Traffic) network are not tested prior to implementation.
- Backup of the Public Works traffic management center (TMC) network are kept only onsite.
- Data center and data room physical and environmental control gaps were identified at multiple locations.

All observations and recommendations noted during our audit are further detailed below. Additionally, these items have been communicated to management.

#	Process/Procedure	Observation	Recommendation	Management Response
1	A Continuity of Operations Plan (COOP) exists for the City of Springfield and includes concept of operation, mission-essential functions, activation and relocation, alternate facility operations, reconstitution, communication plan, test, training and exercises.	**Observation:** The COOP plan was last updated in 2016 and testing of the plan has not occurred on an annual basis. **Risk:** Disruptions of the City's services.	Review, update and test the plan on a periodic basis (at least annually) to ensure the best possible plan with timely recovery.	**Information Systems Network Manager** We will review, update, and test the COOP plan on an annual basis. Target implementation date: July 2020

#	Process/Procedure	Observation	Recommendation	Management Response
2	User access reviews are performed on an ad hoc basis by the following departments: • Environmental Services • Public Works (Traffic) • IS (for domain and enterprise admin) • Parks These reviews are not documented.	**Observation:** Periodic user access reviews are being performed, but not documented. **Risk:** Unauthorized access to critical systems.	Work with Information systems to ensure that periodic (at least annual) user access reviews are performed and documented. Document the following items as part of the review: • Who performed the review • Approval of the review • Action taken for any changes made during the review	**Environmental Services Control Systems Specialist** Environmental Services will conduct an annual review of user access to the SCADA, PLC, & LIMS systems following IS protocol. **Public Works Traffic Professional Engineer** Access reviews that were ad hoc are now scheduled with City and MoDOT administration every six months beginning November 2019. **Information Systems Network Manager** IS will review and identify inactive IS accounts. IS will also provide each department with a list of Active Directory accounts. **Parks Business Systems Analyst** Parks has started documenting user profile changes made by the system administrator as well as changes to Active settings on a spreadsheet. User profile access reviews will now be documented. Target date for implementation not otherwise noted: April 2020

#	Process/Procedure	Observation	Recommendation	Management Response
3	Logical Access is controlled to systems through the new hire and terminations process. The business processes that users have access rights to should correspond with their job functions.	**Observation:** The Senior Database Administrator has system administrator access to the Oracle application, and also has the ability to install, design, migrate data, and configure data within the Oracle database (as a database administrator). **Risk:** Unauthorized program or data changes and the deletion of the evidence of those changes.	Limit the system administrator's access to the application or the database in order to eliminate the segregation of duties conflicts. If limiting access is not possible, ensure logging is in place, and perform a review of the access log on a periodic basis.	**Information Systems Network Manager** Information Systems separated the administrator access as recommended. Implemented: December 2019

#	Process/Procedure	Observation	Recommendation	Management Response
4	We evaluated password configuration and parameters across the City.	**Observation:** A formal written password policy was not in effect for the City. The Oracle database was not configured to enforce password parameters. Minimum password age for SCADA was "0". Password history (passwords that cannot be reused) was: • Zero for the SCADA system at Environmental Services • Five for Public Works (Traffic) network • Five for Active, the Parks application **Risk:** Password parameters across systems and applications should be configured to prevent the risk of unauthorized access.	A formal written password policy should be created and implemented, based on best practices, and password settings should be adjusted to best practices across the various networks and applications as noted below: • Password expiration of 90 days • Password History – should be 8-24 passwords remembered • Minimum password length – 8 to 12 characters • Minimum password age should be at least 1 day • Account lockout threshold should be 3-5 invalid logon attempts	**Information Systems Network Manager** Information Systems is creating a formal written password policy for the City. Implemented: March 2020 Additional responses: **Environmental Services Control Systems Specialist** Environmental Services will adapt procedures to follow the City's formal password policy for the SCADA system once the City's policy is put in place. **Public Works Traffic Professional Engineer** Password history has been modified from 5 to 10 passwords. **Parks Business Systems Analyst** Parks has submitted an enhancement request to Active asking for a password rule change. This change can only be made at the Active level.

#	Process/Procedure	Observation	Recommendation	Management Response
5	Patches for servers and computers in the City's network and are tested and approved prior to deployment.	**Observation:** We reviewed a sample of 10 computer patches and found that four patches were not fully deployed and followed up on in a timely manner. This resulted in 61 machines were not being patched in a timely manner. Discussions for how to better follow-up on patching have been occurring since the week of August 12, 2019. **Risk:** Failure to apply critical patch updates increases the risk the machine will be vulnerable to exploits and attacks.	Establish a follow-up review for failed patching for machines on the network. This will ensure patches are fully deployed in a timely manner.	**Information Systems Network Manager** Information Systems created a review process for patches and performs it on a weekly basis. Implemented: December 2019

#	Process/Procedure	Observation	Recommendation	Management Response
6	Physical access to the main data center and the Environmental Services SCADA office is controlled by badging systems. Personnel are required to swipe the badge before the badging system will allow access into the restricted areas. Parks department switches are in switch closets and are accessible by fulltime employees.	**Observation:** Access to restricted areas via badging systems and physical keys were as follows: • Access via the badging systems to the main data center and the Environmental Services SCADA office were not limited to only individuals who required access based on job responsibilities. A request to reduce the access for the SCADA office, was submitted during fieldwork • Workforce Development partners and vendors are escorted to the data closet, but, partners and vendors' activities within the closet are not monitored • Parks department switch closets were not limited to IS personnel **Risk:** Unauthorized access to data, hardware, and potentially the network.	Limit physical access to data centers and rooms to only those who require access for job responsibilities to ensure protection of data and hardware assets.	**Information Systems Network Manager** Information Systems has corrected the access to the main data center and SCADA office. Access is now limited based on job responsibility. **Workforce Development Computer Support Assistant** Workforce Development has implemented a sign-in sheet for both switch closets in addition to the physical controls already in place. **Parks Business Systems Analyst** Parks will work with IS to secure the switch closets and limit access to authorized personnel. Implemented: March 2020

#	Process/Procedure	Observation	Recommendation	Management Response
7	Patch management for Public Works (Traffic) is occurring on a periodic basis.	**Observation:** Patches are not tested prior to implementation on the Public Works (Traffic) network. **Risk:** Possible loss of information, unexpected or undesirable system behavior, and possible breaches of information.	Work with the Network Manager to facilitate testing of patches prior to implementation into the Public Works (Traffic) network.	**Public Works Traffic Professional Engineer** Public Works will work with IS to ensure patches are tested prior to being applied. Target date for implementation: July 2020
8	The Public Works (Traffic) Network traffic management domain server is backed up daily.	**Observation:** Backups of the traffic management center Public Works (Traffic) Network are kept in the same location as the server. **Risk:** Destruction of the live data and backup in the event of an emergency or disaster.	Work with the Network Manager to facilitate offsite backups to ensure recovery of data and configurations for the domain server.	**Public Works Traffic Professional Engineer** Backup storage is currently maintained offsite. Implemented: October 2019

#	Process/Procedure	Observation	Recommendation	Management Response
9	Data centers and closets are maintained by multiple departments across the City.	**Observation:** Physical and environmental controls differ among data centers and closets throughout the City. See the appendix for specific details. **Risk:** Loss of data, hardware, or unauthorized network access.	Implement additional physical and environmental controls at the identified locations. Work with Information Systems to implement a standard set of controls for data centers and rooms across the City.	**Information Systems Network Manager** Information Systems will work with departments to implement a standard set of controls for data centers and rooms across the City. Target implementation date: July 2020 Additional responses: **Environmental Services Control Systems Specialist** Search for a temporary secure location with the addition of a camera and HVAC dedicated controls is being reviewed by the Plant Superintendent and Control Systems Specialist until a permanent solution is found. Temporary relocation should be completed by March 2020. **Public Works Traffic Professional Engineer** Two network cameras have been installed in the server room with local and remote storage of video.

Appendix: Data Center Controls

Below we've provided a chart of controls for each data center or data room we visited. Note that if a location does not have an "x" it lacks the listed physical or environmental control.

Location	Fire Suppression	Environmental Controls - HVAC	UPS	Camera for Data Center/Closet	Generator
Main Data Center	X	X	X	X	X
Public Works (Traffic) – Data Center		X	X		X
Environmental Services – Data Room			X		X
Emergency Communications – Data Center	X	X	X		X