City of Springfield

IT General Controls – Physical Security

January 31, 2022

BKD
CPAs & Advisors

Contents

Report Letter 1

Executive Summary 2

Recommendations 3

BKD
CPAs & Advisors

201 N. Illinois Street, Suite 700 | P.O. Box 44998 | Indianapolis, IN 46244-0998
317.383.4000 | Fax 317.383.4200 | bkd.com

Report Letter

Mr. David Holtmann, Director of Finance
City of Springfield
218 E. Central
Springfield, MO 65802

We are pleased to provide our report on the IT General Controls – Physical Security performed by **BKD, LLP** (BKD). We want to thank City of Springfield's (the City) management and staff members who contributed positively to our efforts.

We have performed the procedures enumerated in the Executive Summary of this report, which were agreed to by you pursuant to our scope letter, dated November 18, 2021. This engagement was not an audit and was not designed to provide assurance over the prevention or discovery of errors, misrepresentations, fraud, or illegal acts. Inherent limitations in any internal control structure are that errors, fraud, illegal acts, or instances of noncompliance may occur and not be detected. Controls may become inadequate because of changes in conditions or deterioration in design or operation. Two or more people may also circumvent controls or management may override the system.

We were not engaged to provide an opinion with respect to the effectiveness of your controls or degree of compliance with your policies and procedures or applicable laws and/or regulations. Accordingly, we do not express such an opinion. Our procedures were performed on an interview basis only with limited validation and cannot be relied upon to detect all errors or violations of laws, regulations, or City policy. Had we performed additional procedures, other matters might have come to our attention that would have been reported to you. Our report is intended for use only by management of the City, solely for reporting findings with respect to the procedures performed by us.

This report is not intended to be, and should not be, used by anyone other than the specified parties.

BKD, LLP

BKD, LLP

January 31, 2022

Executive Summary

We are pleased to provide our report on IT General Controls (ITGC) – Physical Security performed by **BKD, LLP** (BKD) for the City of Springfield (the City). The overall objective of this engagement is to assist the City with completing the internal audit plan for the year.

The objectives, scope, and procedures we developed, management approved, and we performed are included in the Scope and Procedures Section. The results of our procedures were discussed with management at the conclusion of our engagement and are included in the Results Section.

Background

The National Institute of Standards and Technology (NIST) offers guidelines on technology-related topics such as physical security. NIST guidelines are recommended for government agencies and considered best practices. Section 3.10 of the NIST SP 800-171 describes physical security as measures designed to deny unauthorized access to facilities, equipment, and resources and to protect personnel and property from damage or harm.

The City relies on a combination of physical security elements, such as keys/locks and electronic controls, such as card readers. Physical keys and locks are not susceptible to electronic failures as with electronic controls, but there is a risk of loss or undetected transfer to unauthorized individuals. Electronic locks are typically configured to maintain audit logs and provide an efficient means to terminate a lost badge, reducing the risk of unauthorized access. Physical locks can be inadvertently left unlocked where an electronic lock systematically locks upon closure, again reducing the risk of unauthorized access.

The cost differential between physical keys and electronic locks can be substantial. Different locations, assets, and areas have varying degrees of risk. Deciding on which physical security element to deploy should be based on the associated inherent risk of the assets being protected, the potential impact of threats, and the likelihood of occurrence.

Scope and Procedures

Our procedures included the following:

1. Obtained formal policies and procedures related to physical access security controls, including badges, keypads, access readers, scanners, and keys. Assessed for appropriateness.
2. Conducted interviews with personnel responsible for provisioning physical access and walked through the processes and controls related to the following:
    a. Authorization and approval of provisioning access to sensitive areas for everyone, including employees, contractors, maintenance crew, janitorial, visitors, and others. Documented how these processes differ between employees and non-employees.
    b. Inquired and documented the process for deprovisioning access. Assessed for appropriateness.
    c. Inquired and documented the frequency of periodic access reviews. Assessed for appropriateness.

d. Gained an understanding of additional restrictions related to physical access controls in each area, for example, time frames and days of the week (*e.g.*, both during normal business hours and at other times, such as after hours when an area may be unoccupied).

e. Inquired and documented the frequency and triggers for changing locks, passcodes, etc.

f. Understood the frequency of access reviews and reviewed the results of these access reviews.

3. Obtained an inventory listing of all access controls to sensitive areas (physical locks, keypads, badge readers, scanners, etc.).

4. Inquired and documented the departmental owners responsible for approving access to their areas.

5. Obtained Access Control Listings (ACL) showing all active accounts for each access control.

6. Performed limited testing on the ACL to validate that listed users have been appropriately authorized and are appropriately included.

7. Evaluated the design of controls and documented gaps or opportunities for improvement noted during walk-throughs.

8. Provided management with a written report, which includes:

   a. Results of our procedures

   b. Observations and recommendations resulting from our work

   c. Management responses

Our procedures did not include an assessment of facility security planning or construction, natural disasters, emergency response preparedness or controls such as closed-circuit television monitoring.

Results

As it relates to the City's ITGC – Physical Security, BKD's limited procedures and scope of work resulted in the following recommendation for management's consideration.

Recommendations

Recommendation 1: Assess the Risk to Data Closets

Data closets throughout the City house critical IT hardware and network infrastructure. Some have electronic locks on the doors; however, the majority still have a physical lock and key system. Data closets are inherently a higher risk for possible disruption or impairment of essential services. A security gap in physical access controls of the data closets could create an opportunity for unauthorized access to hardware or systems to introduce a virus or malware into the network.

Unlike electronic locks, a physical key does not allow for proactive monitoring of access to the data closets to monitor appropriateness. Unauthorized access to sensitive data and infrastructure could go undetected in these instances. Management should evaluate the higher-risk data closets and consider upgrading the physical security to electronic locks as determined by an assessment of risk. Doing so may provide the ability for improved monitoring and tracking.

Management Response

Management agrees with the observation.

The City has funded a project to convert all of the lock and key data closets to card reader access. The project was initiated in February 2022 and is estimated to be completed by August 2022. All new data closets are required to be installed with card access.