City of Springfield

IT General Controls – Backup and Recovery

January 31, 2022

BKD
CPAs & Advisors

Contents

Report Letter 1

Executive Summary 2

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 – Backup and Recovery 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) – Backup and Recovery 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

In 2018, the City's primary domain controller went off-line, and the backup controller also failed. As a result, many of the City's critical systems could not authenticate against Active Directory until the domain controllers were rebuilt. During the January 2020 risk assessment, concerns were raised by several system owners about the recoverability of their data should this occur again. At the time of the risk assessment, a formal backup and recovery policy was not provided, and a key leadership position, Director of IS, was vacant. These risk factors, combined with the inherent risk of technology in general, resulted in this project being included on the City's annual internal audit plan.

In February of 2020, a new Director of IS joined the City. The IS department has an annual budget of $4.45M, or 5 percent of the general fund budget. The IS team supports close to 134 software systems and serves over 2,300 employees across 19 departments with operations in over 135 City facilities. There are 31 positions within the IS Department, and two positions remain unfilled.

Scope and Procedures

Our procedures included the following:

1. Obtained and read policies and procedures for the City's backup and recovery processes.
2. Conducted walk-throughs of the processes and controls relied upon for the successful recovery of data, transactions, and programs should a need occur.
3. Evaluated the design of controls and documented gaps or opportunities for improvement noted during walk-throughs.
4. Inquired about and documented the types of backups performed and the media relied upon to assess appropriateness.
5. Obtained backup schedule for critical systems and tested a sample of one to validate existence.
6. Documented retention periods for each type of backup. Assessed for appropriateness and for compliance with formal policies.
7. Inquired and documented the physical storage of all backup types for key systems.
8. Obtained evidence of backup activity to confirm occurrence and successful completion.
9. Performed a test of one (of each type of backup) by requesting and obtaining evidence of backups on sampled dates.

10. Selected one failed backup and validate the timeliness of response. Validated and documented the next successful backup of the same failed instance.

    a. No failed backups were identified for testing.

11. Determined if restoration processes exist and obtained evidence of the most current of restoration testing performed. Tested for compliance with formal policies.

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

    a. Results of our procedures

    b. Observations and recommendations resulting from our work

    c. Management responses

Results

As it relates to City's ITGC – Backup and Recovery operations, BKD did not identify any observations related to our limited procedures and scope of work. We did, however, note significant progress in the overall IS control environment as it relates to backup and recoveries operations.

Improvements important to highlight:

- The City's backup and recovery approach is implementing and following the 3-2-1 Rule. This means that: 1) three copies of data are maintained, 2) on two different storage types, and 3) one copy is maintained off site. The federal agency, Cybersecurity and Infrastructure Security Agency (CISA), a component under the Department of Homeland Security (DHS) recommends this strategy as a best practice.

- The IS Department has created a comprehensive inventory of 134 systems associated with critical government services. This is referred to as the Red Card and published internally. The categorization further indexes each system by:

    - Service impact to the City's operations and potential impact to public safety (*e.g.*, life threatening, non-life threatening, etc.). This assists with determining backup and recovery priority, as well as how best to deploy resources should an incident occur.

    - Sensitivity of the data generated or processed by the systems (*e.g.*, PII, PHI, etc.)

    - Impact due to disruption (*e.g.*, internal, public)

    - Location of the system (*e.g.*, on-premise, cloud or other)

    - Service description of the system as well as function

  An inventory of this type is considered best practice and an essential component of an effective Disaster Recovery Plan (DRP).

- The City has made investments in upgrading essential technology that improves backup and recovery controls, such as:
    - Gartner Magic Quadrant Backup and Recovery Solution is being used to back up all virtual servers. As a result, they capture a point-in-time copy (full backup) and write the data out to a secondary storage location for the purpose of recovering this data in case of loss. Previously, the City relied only on snapshots and incremental backups.
    - Migration to a new data center is currently underway and estimated to be completed at the end of the fiscal year.