TECHNOLOGY & INNOVATION
DISASTER RECOVERY
AND BUSINESS CONTINUITY PLANNING
AUDIT 19-18
DECEMBER 17, 2019

CITY OF TAMPA

Jane Castor, Mayor **Internal Audit Department**

Christine Glover, Internal Audit Director

December 17, 2019

Honorable Jane Castor
Mayor, City of Tampa
1 City Hall Plaza
Tampa, Florida

RE: Disaster Recovery and Business Continuity Planning, Audit 19-18

Dear Mayor Castor:

Attached is the Internal Audit Department's report on Disaster Recovery and Business Continuity Planning.

We thank the management and staff of Technology & Innovation Department for their cooperation and assistance during this audit.

Sincerely,

/s/ Christine Glover

Christine Glover
Internal Audit Director

cc: John Bennett, Chief of Staff
Dennis Rogero, Interim Chief Financial Officer
Russell Haupert, Chief Technology Officer
Eric Hayden, Infrastructure Services Manager

TECHNOLOGY & INNOVATION
DISASTER RECOVERY AND BUSINESS CONTINUITY PLANNING
AUDIT 19-18
DECEMBER 17, 2019

/s/ Stephen Mhere

Auditor

/s/ Christine Glover

Audit Director

TECHNOLOGY & INNOVATION
DISASTER RECOVERY AND BUSINESS CONTINUITY PLANNING
AUDIT 19-18

BACKGROUND

The ability of the City of Tampa (COT) to provide services to citizens and employees on a continuous basis depends on the ability of its technology infrastructure to support operations during and after disasters or other disruptive events. As such, the Technology and Innovation Department (T&I) has implemented a disaster recovery and business continuity (DR/BC) program with the objective to enable operations to continue as smoothly as possible during disasters. Guidance for this is provided in the Continuity of Operations Plan and Emergency Preparedness Disaster Recovery Plan for T&I Infrastructure (COOP & EPDR).

As part of the DR/BC program T&I maintains two reciprocal backup data centers: they are designed such that in certain circumstances the secondary data center can backup the primary while in others, the reverse is true. Hardware and software installations at the two data centers cost approximately $5 million per year. Both of the data centers are equipped with sufficient computing infrastructure to enable critical operations to continue with one of them inoperative. As of July 2019, 12 T&I employees (13 if one senior network engineer position is filled) led by two systems analysts were responsible for DR/BC operations. Operational leadership of DR/BC is the responsibility of the infrastructure manager.

STATEMENT OF OBJECTIVES

This audit was conducted in accordance with the Internal Audit Department's FY 2019 Audit Agenda. Its objectives were to determine if:

1. Internal controls for information technology (IT) service continuity have been implemented to provide reasonable assurances that COT services will continue with minimal disruption during a disaster.

2. T&I implemented best practice standards in the design and setup of its DR/BC practices.

3. Sufficient testing of the DR/BC plan has been done to enable an assessment of the secondary data center's readiness as back up for the primary site.

4. Sufficient testing of the DR/BC plan has been done to enable an assessment of the primary data center as a backup for the secondary site.

5. Employees with DR/BC responsibilities receive necessary training on an ongoing, regular basis.

STATEMENT OF SCOPE

The audit covers FY 2018 and 2019. Prior periods were also included if there were any DR/BC activities undertaken that have or may have direct relevance to audit objectives. Disaster recovery activities related to hosted solutions were not included in audit scope – they run on proprietary hardware and software applications and DR/BC responsibilities lie with the third parties. Also excluded from audit scope are T&I's backup and recovery processes – they were covered in Audit 14-08 (Backup and Recovery).

STATEMENT OF METHODOLOGY

We performed reviews of literature and/or relevant documentation as follows:

- T&I's disaster recovery plan, to evaluate its main elements against best practice standards of the Information Technology Infrastructure Library (ITIL[1])'s IT Service Continuity Management.

- Primary and secondary data center building designs, to assess their compliance with Florida building codes.

- Hillsborough County emergency management information, to determine both data centers' flood and evacuation zone classification.

We toured and inspected both data centers to determine if critical ITIL recommended internal controls were in place. We verified by observation the presence of disaster preventive measures, including the use of redundant power sources in the form of backup power generators. We inspected data center facilities as well as server rooms for physical security. We verified that server rooms at both facilities are ventilated and kept at cool ambient temperatures. We evaluated detective controls for server rooms, including generation of system logs for all entries, use of surveillance cameras, and use of temperature and flooding alert systems.

We interviewed the infrastructure services manager, who is in charge of the DR/BC plan. He provided his perspective on internal controls in the DR/BC function, updating protocols for the DR/BC plan, business impact analysis, and T&I's approach to recovery time objectives. We also explored fraud related to IT service continuity management.

We also interviewed the lead systems analyst responsible for Windows and Linux servers, and the lead systems analyst in charge of database management and mainframe operations. The subjects of our discussions with the analysts included server replication technologies in use at the data centers and recovery point objectives. We also discussed design characteristics of server rooms that act as controls to mitigate against temperature fluctuations, flooding, and other physical damage to critical computer equipment. We also discussed geographical proximity of the two data centers. We also obtained information from engineers in Facilities Management regarding building codes and hurricane classification of data center buildings.

We obtained and reviewed DR/BC team records relating to various activities carried out to test the effectiveness of the disaster recovery plan.

STATEMENT OF AUDITING STANDARDS

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[1] ITIL (Information Technology Infrastructure Library) is an international framework of best practices for delivering IT services.

NOTEWORTHY ACCOMPLISHMENTS

Below are some of T&I's notable accomplishments in DR/BC:

1. T&I adopted Network Attached Storage (NAS) technology that permits seamless failover and failback procedures between data centers and departmental and user computers. As a result, recovery time objective has improved to minutes instead of days and recovery point objective to hours instead of weeks. Also, NAS technology allows users to do their own data restoration from a choice of 63 different restore points.

2. T&I has also virtualized about 98% of COT's data center, enabling server replication technology. This has greatly benefited the disaster recovery of the COT's mission critical public safety servers: cross data center replication allows successful failover of Police servers to the primary data center in less than 15 minutes.

AUDIT CONCLUSIONS

Based upon the test work performed and the audit findings noted below, our conclusions are as follows:

1. Internal controls for IT service continuity have been implemented to provide reasonable assurance that City services will continue with minimal disruption during a disaster. However, additional measures are needed to mitigate vulnerabilities that still exist in some areas.

2. T&I has implemented best practice standards in its DR/BC practices. However, there are areas where improvements can be made, such as the proximity of data centers to each other and protection of servers from physical damage.

3. DR/BC plan tests have been performed to enable an assessment of the secondary data center's readiness as back up for the primary site. However, while testing cannot cover all possible scenarios, cyberattack scenarios have not been tested.

4. DR/BC plan tests have been carried out to assess the readiness of the primary data center as a backup for the secondary site. However, cyberattack scenarios have not been tested.

5. Employees with DR/BC responsibilities have not received necessary training on an ongoing basis. However, opportunities were taken to use DR/BC plan testing as a means to achieve training goals.

DOCUMENTATION AND DISSEMINATION OF POLICY

STATEMENT OF CONDITION: T&I is responsible for COT's IT service continuity management. The function encompasses the use of IT infrastructure in not only disaster recovery operations but also business continuity management. The department endeavors to adopt a high state of readiness to respond to events that may hinder its ability to provide IT services. It does so in many different but complementary ways, the most important of which are the establishment of a data backup program, maintaining two data centers, and keeping a DR/BC plan.

T&I continually updates the COOP & EPDR plan. We reviewed the current plan and found that it contains most elements of best practice standards for effective DR/BC planning. However, business impact analysis and risk assessment, critical elements that form the basis of important disaster recovery decisions, have not been undertaken. Also, the COOP & EPDR plan contains some policy aspects of DR/BC, but it does not address others that are important to the function.

CRITERIA: COT ordinance Section 2-46 requires City departments to document and maintain their respective policies: they make employees aware of their responsibilities. According to ITIL, policy setting is the first and foremost activity in the lifecycle of IT service continuity management.

CAUSE: The DR/BC Plan includes some, but not all, of the information that might be included in its underlying policy. This might have precluded the documentation of a separate DR/BC policy.

EFFECT OF CONDITION: IT service continuity management is a critical yet complex function with a multiphase lifecycle. Without policy guidelines, implementation of disaster recovery and business continuity activities might not be effective, compromising the COT's ability to recover from disruptive events.

RECOMMENDATION: We recommend T&I document and disseminate a DR/BC policy. Among other things, the policy should communicate DR/BC objectives and include a requirement to test the COOP & EDPR plan against all plausible disruptive scenarios on a periodic basis.

MANAGEMENT RESPONSE: We concur with the recommendation. Annually, we modify the plans as new technology and methods replace outdated systems. The previous formats included internal policy sections but these policy statements were not complete enough to stand alone by themselves outside the document. We will update and publish a standard DR/BC policy.

TARGET IMPLEMENTATION DATE: January 1, 2020.

GEOGRAPHICAL PROXIMITY OF DATA CENTERS

STATEMENT OF CONDITION: T&I operates two data centers, one a primary data center leased from a private organization and the other an alternative site owned by COT. The two sites use 'mirroring' technology to execute the backup strategy: if the primary center is disrupted, the secondary is activated to continue operations for server-hosted applications. For applications hosted on the mainframe, operations are restarted from backup tapes kept at an offsite storage location. According to T&I, approximately $2.5 million has been invested in computer hardware and software at each of the data centers. On average, COT pays about $11,100 per month to lease the primary site. The 3-year lease is up for optional renewal on November 1, 2019.

The two data centers are very close to each other: both are located in Tampa and are only three miles apart. In our review of best practices we found that distance between alternative data centers is a strategic factor in disaster recovery. Geographical proximity is desirable for easier and timely relocation of resources between alternative sites during a disaster. However, the closer data centers are to each other, the more likely it becomes that they will be impacted simultaneously by a single event.

We also found in our research that Florida is vulnerable not only to hurricanes but also to tornadoes caused by hurricane weather systems. Tornadoes also have the capacity to cause widespread destruction as well. These are important factors to consider in the process to decide the geographical location of a secondary data center relative to the primary site.

CRITERIA: According to ITIL's best practice standards, data center facilities need to be located separately and far enough away from each other so that the likelihood that both of them will be adversely affected by a single disruptive event is minimal.

CAUSE: The primary data center is located in a building designed to withstand major (Category III) hurricane conditions. Its geographical proximity to the alternative site makes logistical sense in terms of disaster recovery or business continuity (DR/BC) resource relocation planning.

EFFECT OF CONDITION: Both the primary and secondary data centers are vulnerable to disruption by a single event. In the event of such a disaster, the COT's IT operations may be unable to recover quickly enough to support the provision of critical services.

RECOMMENDATION: We recommend T&I consider relocating one of the data centers so that the two sites are far enough away from each other to minimize the likelihood of both being impacted by one disaster.

MANAGEMENT RESPONSE: We understand the finding and agree that it is desirable for an organization to maintain backup data centers apart as far as affordably possible to mitigate even remote risks of dual loss in a regional scale event. Although the risk of two hardened data centers complete with redundant backup power are impacted by the same event is uncommon, it can occur. As such, we will notify leadership of the recommendation and enter a project for funding approval. As soon as we receive notification of approval to proceed, we will provide an implementation date.

TARGET IMPLEMENTATION DATE: 10/1/2020. Receive funding response only. Implementation date to follow an approval.

PROTECTION OF SERVERS FROM PHYSICAL DAMAGE

STATEMENT OF CONDITION: COT's primary and secondary data centers meet most best practice standards for the security and good upkeep of server rooms. They are both secure facilities with guarded reception areas where visitors are required to check-in and cannot enter the facilities unaccompanied. Only authorized personnel can access the server rooms and can only do so using smart cards. Both server rooms are windowless, have no more than two access entrances, are maintained at cool ambient temperatures, and are equipped with temperature sensors that trigger alert messages when ambient temperatures are exceeded. Both data centers have power redundancy: each has two generators that immediately restore power to the data centers during periods of outage.

During our tour of the two sites we made observations that are not consistent with best practice standards for data centers. The observations are as follows:

a) The primary data center is a colocated facility providing server space for three entities, namely COT, the host, as well as another organization. We observed that the host installed a fencing barrier around its servers to provide an extra layer of physical security around them. COT's servers do not have that extra protection.

b) Also at the primary site, servers, network cables, and other computer equipment are mounted on racks with open side panels.

c) Server rooms at both sites are located on the 1st floor. At the primary site, the room has floor water sensors that trigger alerts when they detect flooding. The room also has a pump that automatically removes water from the building. However, at the secondary site, the room has neither floor water sensors nor a pump.

We reviewed publicly available Hillsborough County emergency management information and found that both data centers are located in low to moderate flood risk areas. However, the primary site is located in an evacuation zone: it is in an area assessed to be vulnerable to potential storm tide heights of up to 31 feet. The secondary site, on the other hand, is not in an evacuation zone.

CRITERIA: According to ITIL, the location of major equipment rooms is an important aspect of data center environmental architectures and standards. Also, wherever possible, appropriate risk responses should be implemented to reduce the impact or likelihood of risks from manifesting themselves. In the context of IT Service Continuity Management, these include the risks of sabotage or accidental damage.

CAUSE: Various physical measures implemented to protect the data centers have created a sense of adequacy for the security of servers.

EFFECT OF CONDITION: The lack of floor water sensors and a pump in a first floor server room leaves servers vulnerable to flooding damage. The lack of fencing or similar barrier for servers leaves them vulnerable to physical contact by employees and associates of the other two entities with whom COT shares the server room. While these employees are authorized to enter the server room, they are not authorized to be in physical contact with the City's IT equipment. Open racks leave cables exposed, increasing the risk of their accidental or malicious disconnection from servers. Such disconnection results in server inaccessibility due to loss of network connectivity, causing processing delays or stoppages in the provision of services.

RECOMMENDATION: We recommend T&I consider the following:

a) Erecting fencing or other physical security barrier around servers at the primary site. This will mean that only authorized COT employees can have access to the servers, thereby reducing the risk of damage to them.

b) Installing floor water sensor(s) and pump(s) in the server room at the secondary data center to mitigate against flood damage to servers and other computer equipment.

The foregoing recommendations are subject to management decision regarding a separate recommendation we made in this audit to consider moving one of the data centers to increase their geographical proximity.

MANAGEMENT RESPONSE: Following the recommendation outlined in Audit Inquiry 2, we will submit a project estimate to seek approval funding a data center relocation. If we receive indication of administration directing us to move forward with the project, it could affect priorities of the following:

Item a), we understand the recommendation. Co-located tenants benefit having secure perimeters between groups of computer equipment within a shared data center. We will move forward with obtaining estimates for a perimeter and provide options for implementation dates.

Item b), we recently confirmed with Facilities they do not have actively monitored water sensors or sump pumps at that location. We will ask Facilities how to have that addressed and respond back to Audit.

TARGET IMPLEMENTATION DATE: 5/1/2020 for security perimeter installation/decision. 12/31/2019 for water sensors and mitigation pumps installation decision.

DISASTER RECOVERY TRAINING AND TESTING

STATEMENT OF CONDITION: The purpose of disaster recovery planning is to enable organizations to efficiently restore critical business applications and continue operations in a timely manner following a disaster. This is best achieved through proficient handling of technical and procedural aspects of disaster recovery, which depend on effective personnel training and appropriate testing of DR/BC plans.

Our review of T&I's DR/BC testing showed that the department carried out four tests between May 2017 and June 2019. These failover tests[2] involved both primary and secondary data centers and included the email exchange server, virtual servers for Stormwater and TPD operations, and a capacity test for all production servers. T&I also dealt with two disruptive events in 2019 – a video storage hardware failure and a primary storage outage at one of the data centers. No scenario of a cyberattack was tested. There was also no DR/BC training provided. However, according to T&I personnel, although no training documentation was created, the department leveraged testing activities undertaken to simultaneously achieve training objectives.

CRITERIA: ITIL recommends regularly testing DR/BC plans against defined test scenarios and providing personnel involved in the plans with training on how to implement actions for which they are responsible. The US Department of Homeland Security's Cybersecurity and Infrastructure Security Agency recommends testing the disaster recovery plan and advises local governments to mitigate against cybersecurity threats by reviewing and exercising ransomware scenarios.

CAUSE: T&I moved the primary data center from the public library to its current location in the last few years. Although the department managed to perform some testing during this time, relocation activities tied up personnel, making it difficult to schedule DR/BC training.

EFFECT OF CONDITION: The lack of cybersecurity testing, particularly for scenarios involving ransomware, increases the possibility of ineffective handling of such a disruptive event were it to occur. Also, the lack of DR/BC training for personnel assigned specific responsibilities deprives them of the opportunity to horn the skills they will need to more efficiently perform their tasks during actual disasters.

RECOMMENDATION: We recommend T&I do the following:

a) Regularly test and document all tests for the DR/BC plan for different scenarios, including scenarios for cyberattacks (specifically ransomware).

b) Develop a DR/BC training program for relevant personnel and document all training provided.

[2] A failover test is a testing technique that moves operations to back-up systems during a hardware failure and validates a system's ability to handle extra operational processes and data allocated to it during the test period.

MANAGEMENT RESPONSE: We concur with both recommendations: (a) expanding our DR/BC program to cover cyberattack scenario testing; and (b) developing a training program to improve Disaster Recovery and Business Continuity awareness and testing strategies across additional teams.

Since replicating, relocating and recovering application servers and file storage systems are performed successfully hundreds of times per year in modern virtualized data centers, more awareness and practical experience will benefit our response teams facing continually emerging cyber threats.

TARGET IMPLEMENTATION DATE: June 2020