



# City of Chattanooga

Stan Sewell  
Director

INTERNAL AUDIT  
City Hall  
Chattanooga, Tennessee 37402

Ron Littlefield  
Mayor

October 20, 2008

Mayor and City Council  
City of Chattanooga  
Chattanooga, TN 37402

RE: IT Disaster Recovery, Audit 08-07

Dear Mayor Littlefield and City Council Members:

Attached is the Internal Audit Division's report on the Information Services Disaster Recovery Plan.

We thank the management and staff of the Information Services Department for their cooperation and assistance during this audit.

During this audit it has come to our attention that our City may need to address the need for a city-wide business continuity plan. A business continuity plan is essential in addressing the critical business processes of the City. Each City division should be responsible for taking the lead in preparing and maintaining their own business continuity plans. Then these plans will help the Information Services Department in addressing the critical business processes of the City and setting priorities within the IS disaster recovery plan.

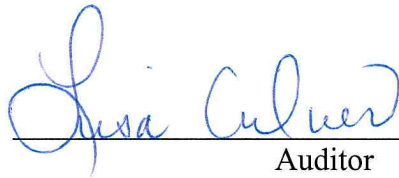
Sincerely,

Stan Sewell, CPA, CGFM  
Director of Internal Audit

cc: Dan Johnson, Chief of Staff  
Mark Keil, Chief Information Officer

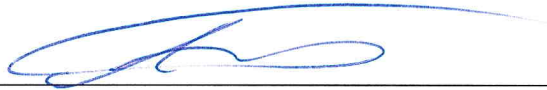
**INFORMATION SERVICES DEPARTMENT  
IT DISASTER RECOVERY PLAN  
AUDIT 08-07  
SEPTEMBER 24, 2008**

**INFORMATION SERVICES DEPARTMENT  
IT DISASTER RECOVERY PLAN  
AUDIT 08-07**



---

Auditor



---

Audit Director

**INFORMATION SERVICES DEPARTMENT  
IT DISASTER RECOVERY PLAN  
AUDIT 08-07**

**INTRODUCTION**

An Information Technology Disaster Recovery Plan is a plan for duplicating computer operations after a catastrophe or any event that causes significant disruption in computer operations for an extended amount of time. The plan should ensure that the critical information systems can be activated at alternate sites in an effective and efficient process. The City's Information Services Department is charged with formulating the City's IT Disaster Recovery Plan and administering it in the event of a disaster. The City's Information Services Department supports 16 departments with approximately 1,400 personal computers. They maintain 6 different operating systems, 60 unique software applications, and 104 servers.

**STATEMENT OF OBJECTIVES**

This audit was conducted in accordance with the Internal Audit Division's 2008 Audit Agenda. The objectives of this audit were to determine if:

1. There is an adequate written IS disaster recovery plan.
2. The Information Services disaster recovery plan is regularly tested and updated.
3. The City's computer facilities (backup sites) are adequate.
4. The data backup procedures are documented and are adequate.

**STATEMENT OF SCOPE**

The scope of the audit is limited to the IS department and the review of their Information Services Disaster Recovery plan, computer facilities and data backup procedures.

**STATEMENT OF METHODOLOGY**

During the audit, auditors reviewed portions of COBIT, researched other audits performed on IT disaster recovery plans, and used the Internet to research disaster recovery plans and governance. Auditors interviewed IS staff concerning their disaster recovery plan. Toured the City's computer facilities and observed the tape retrieval process. Obtained source documentation from IS staff. Original records as well as copies were used as evidence and verified through physical examination. Computer processed data was not used to arrive at our conclusion; therefore, we are not required to assess or attest to the reliability of this type of data.

## **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. In addition, we abide by the standards of professional practice established by the Institute of Internal Auditors. An internal audit charter has not been approved by the City Council.

## **AUDIT CONCLUSIONS**

Based upon the test work performed and the audit findings noted below, we conclude that:

1. The IS Disaster Recovery plan needs updating and enhancement.
2. The IS Disaster Recovery plan is not regularly tested.
3. Some City computer facilities need upgrading and relocating.
4. The IS data backup procedures are not documented.

While the findings discussed below may not, individually or in the aggregate, significantly impair the operations of the Information Services department, they do present risks that can be more effectively controlled.

## **THE IS DISASTER RECOVERY PLAN NEEDS TO ADDRESS THE CITY'S CRITICAL BUSINESS PROCESSES**

A disaster recovery plan should not only emphasize the resumption of information systems, but also focus on the uninterrupted maintenance of critical business processes (business continuity). However, the City doesn't currently have a city-wide business continuity plan (BCP). The BCP would identify those systems that if rendered inoperable would limit the City's ability to deliver vital services and ensure those systems are prioritized logically. Without a city wide BCP, the IS disaster recovery plan can not address the critical business processes of the City or set priorities for reestablishing them in the event of an emergency.

The current plan is out of date and lacks some key components. The City's IS System's staff is currently working on updating the plan and will start reviewing it on a quarterly basis instead of annually. The plan does document some procedures for the department in the event a disaster occurs. It also defines IS teams that would be setup during a disaster and sets their goals.

## **RECOMMENDATION 1**

Based upon control practices within COBIT<sup>1</sup>, to ensure continuous service of the IS department is to first develop an IS plan which would help reduce the impact of a major disruption on key business functions and processes. The plan should include, but not be limited to, identification of critical resources, setting priorities for restoring critical business functions, identifying key personnel and maintaining a current contact list, alternative processing locations, the procedures for backup and recovery, and requiring annual testing and maintenance of the plan. We also recommend that when the City's divisions start the process to establish their own business continuity plan that the IS department work in coordination with them to help set the priorities when restoring the City's critical systems.

## **AUDITEE RESPONSE**

The disaster recovery plan developed by Information Services (IS) deals exclusively with the computer systems of the City and IS will be happy to participate in the development of a citywide Business Continuity Plan.

Information Services has modified their review process of the disaster recovery plan and will be reviewing and making appropriate modification to the disaster recovery plan on a quarterly basis.

## **THE IS DISASTER RECOVERY PLAN IS NOT REGULARLY TESTED**

It is essential to test a disaster recovery plan to determine any deficiencies. It also helps to evaluate the ability of the staff to implement the plan effectively and efficiently. The IS staff does not regularly test the disaster recovery plan. Over the last few years, the IS staff has had to move computer facilities due to the remodeling of City Hall including relocating the City's main computer facility and then fully restoring it at a new location. However, this is not a test of the disaster recovery plan. There are not any scheduled testing requirements included in their disaster recovery plan.

## **RECOMMENDATION 2**

Based upon control practices set by COBIT, testing the disaster recovery plan should be scheduled and conducted on a regular basis, at least annually. The results of the test should be documented and the plan should be updated as needed. The IS disaster recovery plan should set requirements for periodic testing of the plan.

---

<sup>1</sup> IT Governance Institute has established standards issued in COBIT (Control Objectives Management Guidelines Maturity Models). COBIT enables clear policy development and good practice for IT control throughout organizations. ([www.tigi.org](http://www.tigi.org))

### **AUDITEE RESPONSE**

Information Services will develop a procedure to test the disaster recovery plan on a regular basis. The testing process will be monitored and analyzed afterwards. Any problems and issues encountered will be documented and incorporated into the plan.

### **THE CITY'S COMPUTER FACILITIES AND OFFSITE STORAGE ARE NOT STRATEGICALLY LOCATED**

A key component of any disaster recovery plan is an offsite storage location. The offsite storage location should be far enough away that a single event will not result in the destruction of both the computer facility to support daily operations and the offsite storage location. The City's offsite storage location is in the City Hall Annex. Two of the City's computer facilities are located within a few blocks of the offsite storage facility. One is located at the Development Resource Center building (1250 Market St.). While the City's main computer facility is housed in the Pioneer building (801 Broad St.). Both of these locations are within a few city blocks of the offsite storage location.

### **RECOMMENDATION 3**

We recommend the offsite storage location be relocated to a more secure site. We recognize that the site has to be located in an area where IS can still maintain the regular rotation of the media efficiently. The site must also be secure and not comprise the preservation of the media. This may involve additional funding and new technology to improve the security and reliability of the data.

### **AUDITEE RESPONSE**

Information Services will investigate alternate facilities and/or methods for storage of off-site data.

### **SOME CITY COMPUTER FACILITIES ARE NOT FULLY PROTECTED**

To help ensure the continuous flow of the City's business processes and communications, the City's computer facilities must be fully protected and maintained. This responsibility is assigned to the IS Department. Since computer equipment and media storage is very sensitive to its environment and security is always a factor, specific standards must be met to accomplish these tasks. The majority of the City's computer facilities is well protected by fire suppression systems, security cameras, climate monitoring, backup generators and requires authorized access. The City's main computer facility, which is leased from AirNet, is a prime example of a well equipped and fully protected computer site. However, there are a few computer sites that could be considered lacking in protection. The Development Resource Center building houses computer equipment for the occupants of the building in at least two different rooms. Neither room has a fire suppression system or a generator. Only one room is monitored by cameras and has a temperature detection system. Both rooms do require authorized access.

#### **RECOMMENDATION 4**

We recommend that the IS department use the computer facility leased from Airnet to set the standard for all the City's computer facilities in regards to the security, fire protection, and climate monitoring at the minimum in order to protect all the City's computer equipment and sensitive data. This may involve additional funding.

#### **AUDITEE RESPONSE**

Information Services will evaluate each of its computer facilities for deficiencies in the area of security, fire suppression, and climate monitoring and formulate a plan to upgrade any deficient site to sufficient standards.

#### **DATA BACKUP AND TAPE RETRIEVAL PROCESS IS NOT DOCUMENTED**

A critical aspect of maintaining a computer system is to ensure that critical systems and data are adequately and frequently backed-up to protect business operations. A comprehensive set of written procedures which addresses the steps for backing up the City's data and systems, retrieving the tapes and storing them is needed to address this issue. However, currently the IS department doesn't have a complete set of written procedures which details these procedures. IS personnel indicated that they do follow a set standard for data backup and retrieval. A full backup is made of the City's entire system including databases, email and systems every Friday night at each computer facility. These tapes are scheduled to be picked up at each site every Monday and taken back to the City Hall Annex (offsite storage location) to be stored. However, based upon discussions with IS personnel, the full backup tapes are not removed from each site on Monday. The tapes are generally removed weekly, but not always on Monday.

#### **RECOMMENDATION 5**

We recommend that the IS department develop a full set of procedures that addresses the entire process of backing up data, retrieving it and securely storing it. This also includes periodic monitoring of this process to ensure it is being properly followed. We also recommend that IS management work with City management to determine an agreeable risk level set for the acceptable loss of data due to a disaster when setting their procedures for data backup (cost vs. benefit analysis).

#### **AUDITEE RESPONSE**

Information Services will document the process of backup and moving the appropriate tapes off-site. We will also develop written procedures for monitoring the adherence to the established procedures