Internal Audit Report

DEPARTMENT OF TECHNOLOGY AND COMMUNICATION SERVICES DISASTER RECOVERY AUDIT MAY 2008

Office of the County Auditor

OFFICE OF THE COUNTY AUDITOR

Haskell N. Arnold, CPA
County Auditor

May 2008

The County Council and County Executive
of Howard County, Maryland

Pursuant to Section 212 of the Howard County Charter and Council Resolution 22-1985, we have conducted a review of selected activities of the

DISASTER RECOVERY REVIEW
HOWARD COUNTY GOVENMENT

and our report is submitted herewith. The scope of our examination related specifically to a review of Howard County Government disaster recovery plan. The body of our report presents our findings and recommendations.

The contents of this report have been reviewed with the Chief Administrative Officer, and the Department of Technology and Communication Services. We wish to express our gratitude to the various departments for their cooperation and assistance extended to us during the course of this engagement.

Haskell N. Arnold.
County Auditor

Keith N. Zumbrun
Auditor-in-Charge

George Howard Building, 3430 Court House Drive, Ellicott City, Maryland 21043-4392
(410) 313-2005 TTY Number: (410) 313-6401 Fax Number: (410) 313-3287
www.howardcountymd.gov

INTRODUCTION AND SCOPE

We prepared a data assessment questionnaire that surveyed the Department of Technology and Communication Services (DTCS) about the County's data disaster recovery plan. We met with the Director of the DTCS and he and his staff completed the document. We found that while certain crucial functions of the plan are being performed, several necessary components that should be considered and implemented are not being done. We believe that our recommendations below, when implemented, will strengthen the overall County ability to prepare and recover from an unforeseen disaster and interruption in the continuity of the County's service and business operations.

BACKGROUND

A disaster recovery plan is a critical component of a business' ability to continue services and needs to it's customers in the event of a major disaster such as a fire, earthquake, flood, hurricane and even terrorism. The plans purpose is to enable an organization to process data and services while computer equipment is being repaired or replaced and computer files are being reconstructed. File backup on a systematic schedule which is off site is certainly a minimum requirement of recovery. The most powerful backup strategies are those that integrate backup and system recovery tools to ensure that information and systems are accessible wherever, whenever and to whomever the organization deems appropriate. When these tools are used together, organizations can realize immediate benefits which include faster recovery and increased uptime.

There are four components to a disaster recovery plan:

(1) Prevention – this part describes how to protect the system and steps to avoid a disaster to begin with. A complete system of controls is designed based on risk assessment and cost effectiveness.

(2) Contention – since there is no fool proof, fail-safe system, this part identifies how to react and to maintain what is working while the disaster is occurring.

(3) Recovery – this area answers the question, how do we recover and reestablish the system to normal operations.

(4) Contingency – this part details how to keep the systems running and services available to the public until the system is restored. It identifies and describes how the County will operate and conduct business while recovery efforts are taking place.

A determination must be made as to what functions are necessary to keep the county running. Vital functions might be 911 operations, water and sewer systems, property tax systems, accounts receivable, accounts payable, payroll, etc. Copies of these applications, including programs, data, and documentation, should be stored in a secure location off-site. Costs estimates for not performing these functions should be estimated to include legal, moral and public requirements and those associated penalties. Some indirect costs to consider are employee morale and image and should be quantified as part of the decision process. Essentially, the cost benefit question should be considered and answered; if the cost of developing, installing and maintaining the contingency play are less than the costs of not having one, then it should be implemented.

Each critical function should be examined for alternate contingency strategies. A possibility is to ask if could be performed manually and for how long. Another idea might be to outsource the function to an outside company. An example might be the County's payroll with Automatic Data Processing (ADP). Some other alternatives include:

- Howard County owned back-up facility – this would replicate the total system and should be somewhere distant from our main office complex. This option is high costs but low risk because the County maintains total control.

- Reciprocal agreement – This option entails a contract between the County and another entity with compatible systems that would service each other in case of a disaster. This requires all changes between the parties to be communicated as they occur so that compatibility can be determined. Another drawback is the stress placed on the running system to run both companies processing needs.

- Hot Site – This is a backup facility offered by a vendor on a fee basis to users of a particular family of computers. In the event of a disaster, subscribers can use the hot site within 24 hours and for a set duration, usually months. If the disaster is widespread, the hot site may be over taxed as all subscribers will be vying for those resources. The hot site business is dominated by Comdisco and Sungard Recovery Services. The county recently had a contract with Sungard for their mainframe applications.

- Consortium – Several companies get together and build or buy their own facility.

- Service Bureau – Contracting for emergency processing is workable for a short term solution. However, most run their operations at maximum capacity and may not have room for all.

- Shell – this option is a building with all the necessary outlets and connections but no equipment. Equipment and staff are moved to site when needed. Effectiveness for this option is low.

- Mobile Data Center – a system housed in a semi-trailer. Can be manned and maintained 24/7 and ready to roll distances if needed.

In some organizations, both contention and contingency elements are combined into one plan. These plans, separately or together, should contain emergency procedures and operations. Their objective is to handle emergencies in an orderly manner, minimize damage to personnel and assets, and establish an environment for reconstruction and recovery to normalcy. Some specific contention plan elements might be:

- Guidelines for emergency shutdown of the computers system and auxiliary devices
- Location of emergency exits, fire extinguishers and exit procedures
- Emergency lighting and power switch locations
- List of items the employee should take with them
- Contact numbers and location of contingency processing facility
- Employee call down procedure
- List of vital applications and instructions on how to begin processing
- Procedures to make assessment of disaster damage

The contingency plan should be maintained and updated on a regular basis and testing of the plan should be done periodically. Moreover, all personnel responsible for contingency plan activation should also be trained and updated on the same basis. The more testing and updating the smoother the required transition and quicker the enterprise is up and running again. Generally disaster recovery plans are tested one to four times a year. Some of the evaluation criteria should be:

- Were all files and programs available at the off-site facility
- Were JCL, procedure libraries and manuals up-to-date and available
- Was supporting documentation available and complete
- Did the application software load successfully and produce accurate results
- Were the facilities adequate to accomplish the task in a test situation

Findings and Recommendations

We prepared a survey related to disaster recovery and Howard County Government and had the director of the Department of Technology and Communication Services. The survey was answered by various key employees in the department. The survey was a fact finding vehicle to determine what the county had in place in terms of a disaster recovery plan, what the testing intervals and results of the plan were and what policy and procedures were developed, maintained and updated.

The County is far along in the process of migrating from a mainframe provider of services to a server based applications provider. So much so, that they just recently terminated the contract they had with SunGard Recovery Services LP because there is only one application still provided by the mainframe, water and sewer, and that is in the process of being changed to a server platform. The SunGard contract was costing the county about $60,000 annually. We were informed that backup procedures for the DTCS servers are occurring on a regular basis and that the procedures are updated when changes are made. There are generalized procedures that do include versions of the backup software, tape drives retention schedules and Independent Services Corporation in Westminster, MD, serves as the off-site storage location for the backups.

The existing Disaster recovery plan is mainframe based and with the changes mentioned above, is in need of revision to be protect and recovery from the County's sever based applications. The plan needs to be inclusive of all the county's data systems, and to include the previously mention areas that include written policy and procedures, regular and consistent updating of those policies and procedures, regular testing , and that includes the recovery from the hot site and transitioning to normal operations.

In times of scarce resources, setting aside funds and planning time for potential disasters is difficult as there are many issues vying for those resources. However, the set back caused by a disaster to the county could truly cripple our data processing ability and thus most services to Howard County Residents when they are especially needed. A well thought out disaster recovery plan that includes those items discussed above could literally be a life saver, and provide necessary services when they are needed in the most effective fashion. We therefore recommend that:

1. ***The County prepare and maintain a current comprehensive disaster recovery plan that takes into account the items mentioned in this report.***

Administration Response

The Administration concurs with this recommendation. The disaster recovery plan for the County is currently under redesign. Over the past year the Department of Technology and Communications has moved storage and backup solutions from small business applications to Enterprise Architecture. As noted in the audit report our move from mainframe systems to a client server architecture as well as replacement and implementation of multiple applications across the County has warranted a complete redesign of the disaster recovery approach and plan. * Redesigning this plan will follow the following steps. A vendor has been selected and this work is scheduled to begin in June of 2008 with an eight month timeline.

Auditor's Comments

* The Administration attached an outline to the response above that takes into account the various steps and activities needed to accomplish this recommendation. We only included the portion of the response that addressed that a comprehensive plan was needed. The steps outlined in the attachment will in our opinion provide an adequate solution.

KZ:dl-dr07