

Disaster Recovery for Information Technology

March 3, 2007

Special Report #628

Released on : April 6, 2007

SPECIAL REPORT #628

INTRODUCTION - 1 -
BACKGROUND - 1 -
STATEMENT OF OBJECTIVE - 2 -
STATEMENT OF SCOPE AND METHODOLOGY - 2 -
STATEMENT OF STANDARDS..... - 2 -

ATTACHMENT ‘A’

PREVIOUS ERNST & YOUNG “MANAGEMENT LETTER” COMMENTS

ATTACHMENT ‘B’

THE INFORMATION TECHNOLOGY DEPARTMENT’S FULL RESPONSE

OFFICE OF THE COUNCIL AUDITOR
Suite 200, St. James Building



March 3, 2007

Special Report #628

Honorable Members of the City Council
City of Jacksonville

INTRODUCTION

For the past six years, Ernst & Young (E&Y) LLP's management letter to the City of Jacksonville has noted the lack of sufficient disaster recovery preparedness for the City's information technology function. While modest gains such as the installation of a generator at the City's data center have been attained, it is apparent that preparing the City for a disaster, from a technology perspective, has not been a procedural or a funded priority.

BACKGROUND

Subsequent to the end of each fiscal year, the City of Jacksonville (City) has an independent accounting firm (currently E&Y) audit the City's Consolidated Annual Financial Report (CAFR). As part of their audit work, the firm becomes aware of conditions of the City's operating environment where improvement may be warranted. These conditions don't preclude a favorable opinion on the City's financial statements, but they are areas where the independent accountants feel improvement or modification would be beneficial to the City. The "Management Letter" is the collection of the independent accounting firm's observations and recommendations.¹

From fiscal year 1999 – 2000 through fiscal year 2004 – 2005 (six years) the independent accounting firm's management letter has included a comment about the City's level of disaster preparedness. The draft management letter for fiscal year 2005 – 2006 also includes a similar comment. With regard to the observations and recommendations in the management letters, E&Y's concern was focused on the information technology (IT) component of proper disaster preparedness.

We read the prior six management letter comments concerning disaster preparedness and found that they are very similar. The Administration's response varied, but Ernst & Young's comment has appeared, almost unchanged, in each of the past six letters.

¹ See *Attachment A* for a listing of E&Y's comments and the City's responses in the past six management letters.

Through discussion with the Emergency Preparedness Division (EPD) of the Fire and Rescue Department we learned of efforts undertaken over the past few years to ensure that critical agencies had a Continuity of Operations Plan (COOP; continuity plan). A continuity plan “focuses on the operation of the overall organization identifying essential services that must be up and running within 12-24 hours should an event occur.” In 2003, BCP International, LTD (BCPI) created continuity plans for several critical areas: 9-1-1 centers, the Jacksonville Sheriff’s Office, the Fire & Rescue Department, Public Works and the Emergency Operations Center.

Subsequently, additional continuity plans were created for other agencies (including the Information Technology Division, ITD²) within the City of Jacksonville. Simultaneously, BCPI conducted a vulnerability assessment on the City’s technology infrastructure. The vulnerability report and ITD’s continuity plan are both dated December 2004. It is important to impress upon the reader that most any continuity plan, for any agency of the City, places a heavy reliance on technology and therefore a heavy reliance on ITD.

In 2006, the City contracted with URS Corporation to report on the sufficiency of the existing continuity plans. EPD is currently working with URS to act on recommendations from URS’ review.

STATEMENT OF OBJECTIVE

To determine the current state of the Information Technology Department’s disaster preparedness.

STATEMENT OF SCOPE AND METHODOLOGY

We conducted interviews with representatives from both the Information Technology Department and the Emergency Preparedness Division.

STATEMENT OF STANDARDS

This report does *not* represent an audit or attestation performed in accordance with generally accepted government auditing standards.

This report was produced pursuant to Chapter 102 of the Municipal Code of the City of Jacksonville.

² Ord 2006-1194-E reorganized the Executive Branch, removing the Information Technology Division from the Administration & Finance Department, and establishing the Information Technology Department (ITD).

RESPONSES

Responses from ITD have been inserted after the respective observation. As ITD provided additional comments, their full response can be found as *Attachment B*. We received these responses from ITD, via an email dated March 25, 2007.

Observation 1 *Testing / Updating*

Testing of ITD's continuity plan has not occurred. In addition, the plan has had no meaningful update in the past two years.

ITD's continuity plan has no detail in the following significant areas:

Critical Vendor Contact Information
Critical Equipment List

Former employees are still referenced in the document. In addition, because of recent infrastructure technology changes within ITD, the document may be less useful than even the two year time discrepancy would indicate.

ITD's Response

Although there is no documented formal plan, ITD has performed various recovery scenarios with our testing environments. The databases, file systems, and hardware of our most critical systems have been recovered to alternate devices. The COOP study from 2004 has not yet been updated nor its recommendations implemented. This document has been revisited several times over the past two years, but due primarily to more immediate priorities this has not received comprehensive treatment.

Observation 2 *No Disaster Recovery Plan*

ITD's continuity plan makes several assumptions concerning relocation to an alternative site, and then states that no suitable site exists for the relocation of ITD's Network Technologies, Computer Operations and Systems & Programming functions.

Per conversations with the EPD, ITD's continuity plan addresses department operations, staff availability, and temporary staff housing in the event of a disaster. It does not address technology availability. Technology availability is not within the scope of the continuity plan.

Technology availability and recovery should be addressed within a disaster recovery plan (DRP). ITD does not currently have a DRP.

ITD's Response

Generally, we are in agreement with the findings by E&Y and the report generated by the Office of the Council Auditor. ITD has a limited recovery plan that includes the city's most critical systems, but does not have a comprehensive DRP. ITD has taken steps this year to lay the foundation for more resilient systems. We have implemented new hardware standards, increased storage capacity, procured a new backup system, and increased clustering capabilities. The principle of high-availability has been added to the cultural elements of technology architecture.

Observation 3 *Recommendations Not Implemented*

BCPI provided the City with recommendations to rectify vulnerabilities it had identified. Many of these have not been addressed, including:

- BCPI identified that the list of alternate sites was merely a list of names, that these sites were not presently able to provide appropriate accommodations.
- “Until the mainframe is unburdened 100%, a “warm” back-up for it is an absolute imperative.”
- “There is no enterprise wide DRP (disaster recovery plan), in any form. ... Use the resultant fully viable COOP as the analysis phase and prepare an RFP to acquire a complete DRP.”

ITD's Response

BCPI recommendations provided in the 2004 vulnerability report have been addressed:

- Alternative Sites: We have begun informal discussions with other Florida cities and agencies about supplying alternative sites.
- Mainframe Availability: We have implemented a new architecture for the mainframe. We maintain a complete backup of the system that can be fully restored. Current funding constraints have precluded us from investing in a “warm” backup of the mainframe. Since 2004 we have moved many applications off the mainframe, therefore this section of the report will need to be revised to represent current status.
- DRP: ITD has requested through the same grant funding that supplied the vulnerability report, a resource to assist in creating an enterprise DRP. We have requested this the past three grant cycles and the request has been declined each year.

Council Auditor's Rebuttal

We would like it to be clear to the reader that the commencement of informal discussions indicates a very preliminary status and should not be taken as steps that would mitigate an actual disaster.

With more than \$100 million having been spent from the account representing ITD over the last six years, including the rollout of new servers and systems, we fail to see the existence of a funding constraint.

Finally, while we certainly encourage the pursuit of grant funds, grants are often uncertain revenue; something as important as technology disaster recovery should have general budget dollars allocated to it. If grants are realized then additional work could be performed or, in the case of restrictive budgets, the General Fund could be relieved of its obligations.

Observation 4 *Requiring Action*

We were unable to locate any requirement necessitating regular review and updates of the continuity plans and other related disaster preparedness documentation. As noted in Observation 1 above, ITD has not updated its official continuity plan for more than two years. Related literature seems to indicate that plans should be updated at least once a year.

ITD's Response

We agree. This activity must become a higher priority within ITD.

Observation 5 *Recovery Efforts*

The City currently has no cold, warm or hot-site recovery location(s)³ for its IT infrastructure.

The City does not currently have memoranda of understanding (MOUs) with vendors. These MOUs would establish agreements for the rapid procurement of replacement equipment.

ITD's Response

Although official MOUs do not exist, we do have agreements with our major partners to supply equipment in emergencies. These partners include Motorola, Dell, IBM, and Sun. We choose strategic partners partially on their ability to assist in emergency scenarios. We will work to implement formal agreements with our most strategic partners.

Recommendations

Much like premiums on insurance policies, the monies spent on disaster recovery do not typically result in immediate return on investment. Understanding this, one can easily see why it

³ The terms cold-site, warm-site and hot-site, refer to the level of readiness of an alternate data center. Generally speaking, a "hot-site" is a disaster recovery facility that mirrors an organization's production environment and typically has immediate data synchronization. Operational recovery is within minutes of a disaster. Contrast this with a "warm-site," which periodically updates the data at the recovery facility, and a "cold-site" where typically only facilities and some equipment are available.

is more attractive to invest limited resources on upgrades and new systems rather than disaster recovery and continuity.

- We recommend that the Administration provide disaster recovery preparation projects appropriate funding in its 2007 / 2008 budget submission to the City Council. The Administration should not rely solely on grant dollars to fund disaster preparedness activities. ITD should devote sufficient resources to the completion of a disaster recovery plan.
- The Administration should ensure that all continuity and recovery plans are reviewed and, if necessary, updated at least once per year. It may be beneficial to require more frequent review from “critical” agencies.
- We recommend, at a minimum, annual tests of the recovery plan.
- The City’s Risk Management Division should be included in any risk assessment or mitigation exercise.
- As with other aspects of security, it is likely more economical to consider and add disaster recovery processes during the implementation of a new process or system as opposed to after-the-fact. After an initial disaster recovery plan is created, we recommend ITD include additional planning in all future systems development and infrastructure build-outs.

We appreciate the assistance and cooperation we received from the Information Technology Department and the Emergency Preparedness Division through the course of our work.

Respectfully submitted,

Kirk A. Sherman

Kirk A. Sherman, CPA
Council Auditor

Prior Year Management Letter Comments

Fiscal 2000

E&Y Comment

The City is in the process of reviewing its existing Disaster Recovery Plan and evaluating the feasibility of sharing a recovery site with Jacksonville Electric Authority (“JEA”). However, the City has not developed any procedures to address the continuity of its business operations.

In the event of a disaster, the City may not be able to recover critical business and information technology processes in a timely manner. This may adversely affect the City financially.

We recommend the City perform a business impact analysis (“BIA”) to identify critical operational processes. We further recommend that the City use the results from the BIA to develop recovery procedures for critical business processes. Disaster recovery planning should be addressed as part of the Business Continuity Plan.

Once the City has developed a formal Business Continuity and Disaster Recovery Plan, it should test these plans to validate any assumptions made in developing these plans. Further, tests should be performed annually to update the plan for any changes to COJ’s operational and information technology processes.

COJ Response

All current and proposed system initiatives are being driven by the City’s business plan. This requires association with a Tier initiative.

It is not anticipated that a Disaster Recovery Plan will be funded at the current time.

Fiscal 2001

E&Y Comment

COJ is in the process of reviewing its existing Disaster Recovery Plan and evaluating the feasibility of sharing a recovery site with Jacksonville Electric Authority (“JEA”). However, the City has not developed any procedures to address the continuity of its business operations.

In the event of a disaster, the City may not be able to recover critical business and information technology processes in a timely manner. This may adversely affect COJ financially.

Prior Year Management Letter Comments

We recommend that the COJ perform a business impact analysis (“BIA”) to identify critical operational processes. We further recommend that the City use the results from the BIA to develop recovery procedures for critical business processes. Disaster recovery planning should be addressed as part of the Business Continuity Plan.

We also recommend that once the City has developed a formal Business Continuity and Disaster Recovery Plan, it should test these plans to validate any assumptions made in developing these plans. Further, tests should be performed annually to update the plan for any changes to COJ’s operational and information technology processes.

COJ Response

“Preliminary meetings were held in August 2001 with representatives from Sun Guard and EMC to identify the number and styles of processing platforms located in the computer room on the 2nd floor of the City Hall Annex at 220 E. Bay Street.”

Sun Guard maintains strategically located facilities containing specific hardware platforms/operating systems for Customer use when a disaster is declared. EMC is the disk manufacturer used by ITD for enterprise storage. The two companies work together to offer a replication of a Customer’s site for use in a disaster.

Fiscal 2002

E&Y Comment

The City is in the process of reviewing its existing Disaster Recovery Plan and evaluating the feasibility of sharing a recovery site with Jacksonville Electric Authority (JEA). However, the City has not developed any procedures to address the continuity of its business operations. In the event of a disaster, the City may not be able to recover critical business and information technology processes in a timely manner. This may adversely affect the City financially and operationally.

We recommend the City perform a business impact analysis (BIA) to identify critical operational processes. We further recommend the City use the results from the BIA to develop recovery procedures for critical business processes. Disaster recovery planning should be addressed as part of the Business Continuity Plan.

We also recommend that, once the City has developed a formal Business Continuity and Disaster Recovery Plan, it should test these plans to validate any assumptions made in developing the plans. Further, tests should be performed annually to update the plans for any changes to the City’s operational and/or information technology processes.

Prior Year Management Letter Comments

COJ Response

Per Wally Eaton, Chief Security Officer, the City is no longer looking to use the Emergency Operations Center (EOC) in case of an emergency. We continue to evaluate the existing plan. In addition, we are receiving and reviewing proposals from vendors.

Fiscal 2003

E&Y Comment

The City of Jacksonville (City) does not have a Disaster Recovery Plan (DRP), hot site agreement, or a hardware replacement program in place. Last year, City was contemplating a plan with the Emergency Operations Center (EOC). However, the City is no longer looking to use EOC. City is continuing to evaluate a plan and is currently reviewing proposals from vendors. In the event of a disaster, the City may not be able to recover critical business and information technology processes in a timely manner. This may adversely affect the City financially. We recommend that the City perform a business impact analysis (BIA) to identify critical operational processes. We further recommend that the City use the results from the BIA to develop recovery procedures for critical business processes. Disaster recovery planning should be addressed as part of the Business Continuity Plan.

We also recommend that once the City has developed a formal Business Continuity and Disaster Recovery Plan, it should test these plans to validate any assumptions made in developing these plans. Further, tests should be performed annually to update the plan for any changes to City's operational and information technology processes.

COJ Response

Per Wally Eaton, Chief Security Officer, the City is looking into the Emergency Operations Center (EOC) in case of an emergency.

The Information Technologies Division will request funding in the 2004-2005 budget process for an independent business impact analysis to be conducted. While there is not currently a backup site identified, it is ITD's opinion that critical functions could operate in a disaster mode long enough to restore normal processing in the event of a disaster. Provisions such as emergency blanket orders with key vendors, arrangements with banks to produce estimated payroll and vendor payment checks at historical levels, and partnership with the EOC would all contribute to the ability to withstand business interruptions.

Additionally, ITD has recently applied for grant funding to increase the generator capacity of the current data center location. Upon completion of a funded business impact analysis, ITD will begin the process of requesting funding necessary to implement the actions recommended by the study.

Prior Year Management Letter Comments

Fiscal 2004

E&Y Comment

The City does not have a formal Disaster Recovery Plan (DRP), hot site agreement, or a hardware replacement program in place. In the event of a disaster, the City may not be able to recover critical business and information technology processes in a timely manner. This may adversely affect the City financially.

We recognize that the City has contracted for the performance of a business impact analysis (BIA) and development of a continuance of operations plan and is in the final stages of this contract. We recommend that the City use the results from the BIA to develop recovery procedures for critical business processes. Disaster recovery planning should be addressed as part of the Business Continuity Plan.

We also recommend that once the City has developed a formal Business Continuity and Disaster Recovery Plan, it should test these plans to validate any assumptions made in developing these plans. Further, tests should be performed annually to update the plan for any changes to City's operational and information technology processes.

COJ Response

The COOP study has been completed, and ITD has requested and received an extract from that study that be implemented as an action plan prior to conducting a full-scale disaster recovery plan exercise. The ITD management team is currently in the process of assigning responsibilities and target dates for this action plan.

The ITD team has developed a disaster response "kit" consisting of cell phones, laptops, contact lists, key vendor information, key system staffing lists etc. Succession plans and notification escalation lists are also part of this strategy.

Additionally, the ITD management team has received authorization to procure a back-up generator for the City Hall Annex, and is in the process of accessing the funding source to issue the purchase order.

Fiscal 2005

E&Y Comment

The City does not have a formal Disaster Recovery Plan (DRP), hot site agreement, or a hardware replacement program in place. In the event of a disaster, the City may not be able to recover critical business and information technology processes in a timely manner. This may adversely affect the City financially.

Prior Year Management Letter Comments

We recommend that the City use the results from the business impact analysis to develop recovery procedures for critical business processes. Disaster recovery planning should be addressed as part of the Business Continuity Plan. We also recommend that once the City has developed a formal Business Continuity and Disaster Recovery Plan, it should test these plans to validate any assumptions made in developing these plans. Further, tests should be performed annually to update the plan for any changes to City's operational and information technology processes.

COJ Response

The COOP study has been completed, and ITD has requested and received an extract from that study that can be implemented as an action plan prior to conducting a full-scale disaster recovery plan exercise. We have implemented the foundation of a response plan for each affected area. It is our intent to complete 50% of the agencies this fiscal year. Due to time and resource constraints we will not complete a city-wide response plan.

Many steps have been taken to strengthen our enterprise. The Data Center is now on a backup generator that will provide power to all critical systems. ITD also has a close relationship with EOC and we are working jointly to provide technology services in the event of a disaster. Several investments have been made to create hot and cold sites locally. We have also begun to contact other City and County agencies to create a recovery cooperative throughout the State of Florida.

ITD Audit Response: Disaster Recovery Report

Summary

ITD has reviewed the report on disaster recovery from the Office of the Council Auditor. We believe that the information contained in the report is fair and accurate, although it does not fully reflect the accomplishments of this year. ITD is committed to enhancing the recovery and continuity plans for the city technology operations.

We have provided a unified response to the five observations outlined in the report, as well as information regarding the accomplishments, challenges, and barriers in completing a comprehensive emergency and continuity plan.

ITD Responses The table below contains ITD’s comments on each of the audit observations.

Observation	Response
1- Testing/Updating	Although there is no documented formal plan, ITD has performed various recovery scenarios with our testing environments. The databases, file systems, and hardware of our most critical systems have been recovered to alternate devices. The COOP study from 2004 has not yet been updated nor its recommendations implemented. This document has been revisited several times over the past two years, but due primarily to more immediate priorities this has not received comprehensive treatment.
2- No Disaster Recovery Plan	Generally, we are in agreement with the findings by E&Y and the report generated by the Office of the Council Auditor. ITD has a limited recovery plan that includes the city’s most critical systems, but does not have a comprehensive DRP. ITD has taken steps this year to lay the foundation for more resilient systems. We have implemented new hardware standards, increased storage capacity, procured a new backup system, and increased clustering capabilities. The principle of high-availability has been added to the cultural elements of technology architecture.
3- Recommendations Not Implemented	BCPI recommendations provided in the 2004 vulnerability report have been addressed: <ul style="list-style-type: none"> • Alternative Sites: We have begun informal discussions with other Florida cities and agencies about supplying alternative sites. • Mainframe Availability: We have implemented a new architecture for the mainframe. We maintain a complete backup of the system that can be fully restored. Current funding constraints have precluded us from investing in a “warm” backup of the mainframe. Since 2004 we have moved many applications off the mainframe, therefore this section of the report will need to be revised to represent current status. • DRP: ITD has requested through the same grant funding that supplied the vulnerability report, a resource to assist in creating an enterprise DRP. We have requested this the past three grant cycles and the request has been declined each year.

Continued on next page

ITD Audit Response: Disaster Recovery Report, Continued

ITD Responses (continued)

Observation	Response
4- Requiring Action	We agree. This activity must become a higher priority within ITD.
5- Recovery Efforts	Although official MOUs do not exist, we do have agreements with our major partners to supply equipment in emergencies. These partners include Motorola, Dell, IBM, and Sun. We choose strategic partners partially on their ability to assist in emergency scenarios. We will work to implement formal agreements with our most strategic partners.

Successes

The following are high-level accomplishments over the past year:

- New resilient systems architecture
 - All new implementations include recovery documentation
 - High-availability is a requirement on all critical systems
 - Critical systems have been reviewed and action plans created to mitigate discovered weaknesses
 - New tape library and SAN implemented to support recovery efforts
 - New SQL Server, Oracle Server, and Web Architecture being deployed
 - Additional appliances to support global redirection of city Internet traffic
 - Network cores upgraded to provide multiple paths for communication
-

Challenges

The following challenges have impeded progress:

- Funding for recovery planning and technology implementation
 - Lack of human and technology resources
 - Project load
 - Antiquated and inadequate architectures
-

Continued on next page

ITD Audit Response: Disaster Recovery Report, Continued

Data Center

ITD has received preliminary approval and funding commitment to move the data center from its current location in the Hayden Burns City Hall Annex to the Ed Ball Building. This move is planned to occur sometime after October 1, 2007.

The opportunities presented by this move have far reaching impact on our overall business continuity strategy. New uninterrupted power source units are budgeted, as are infrastructure improvements to climate control and data center layout. The location on the fourth floor provides ample protection from rising water, and proximity to the Emergency Operations Center also facilitates rapid deployment of hardware and human resources between the sites.

The facility is being designed as near to a Level 3 data center as can be attained in the facility, with security and redundancy commensurate with a hardened facility.
