TO: The Honorable Chairman and Members of the Board of County Commissioners

FROM: Ken Burke
Clerk of the Circuit Court
Ex Officio County Auditor

SUBJECT: Follow-Up Audit of IT Disaster Planning

DATE: February 10, 2011

For your review and filing in the Official Records, I am enclosing a copy of the follow-up audit dated February 10, 2011 on the above-referenced audit.

I hope you find this report helpful in ensuring Pinellas County government provides the best possible service to our citizens.

cc: Robert S. LaSala, County Administrator
Jim Bennett, County Attorney
Paul F. Alexander III, Executive Director, Business Technology Services
Claretha N. Harris, Chief Deputy Director, Finance Division
Ernst & Young
February 10, 2011

The Honorable Chairman and Members
of the Board of County Commissioners

We have conducted a Follow-Up Audit of IT Disaster Planning. The objectives of our review were to determine the implementation status of our previous recommendations.

Of the three recommendations in the report, we determined that all three were partially implemented. The status of each recommendation is presented in this follow-up review.

We appreciate the cooperation shown by the staff of Business Technology Services during the course of this review.

Respectfully Submitted,

[Signature]

Hector Collazo, Jr., Director
Audit Services, Division of Inspector General

Approved:

[Signature]

Ken Burke, CPA*
Clerk of the Circuit Court
Ex Officio County Auditor

*Regulated by the State of Florida
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Introduction</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>4</td>
</tr>
</tbody>
</table>

**Status of Our Recommendations**

1. No Response Times For Service Levels Are Identified. | 7    |
2. Recovery Time Objectives Are Not Estimated For Disaster Levels. | 10   |
3. No Cost Estimates For Activating A Remote Computer Facility Has Been Included As A Factor. | 14   |

**Appendix A** | 16
INTRODUCTION

Synopsis

The Disaster Recovery Plan is aimed at getting the most important system applications restored after a disaster, but it does not communicate how long it will take or what it will cost. A disaster plan for the computer center is a good start, but needs to be expanded to support the County’s Emergency Management Plan.

Scope and Methodology

We conducted a follow-up audit of IT Disaster Planning. The purpose of our follow-up review is to determine the status of previous recommendations for improvement.

The purpose of the original audit was to:

1) Determine that the Disaster Recovery Plan maximizes the County’s ability to ensure the continuity of business operations in the face of unforeseen events within acceptable budgetary limitations.
2) Determine that the plan was adequately developed, tested, and implemented.
3) Determine how well the Disaster Recovery Plan coordinates with the County’s Emergency Management Plan.

To determine the current status of our previous recommendations, we conducted an interview with management to determine the actual actions taken to implement recommendations for improvement. We performed limited testing to verify the process of the recommendations for improvement.

Our follow-up audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing and Standards for Offices of Inspector General, and, accordingly, included such tests of records and other auditing procedures, as we considered necessary in the circumstances. Our follow-up testing was performed during the month of December 2010. The original audit period was October 1, 2006 through July 31, 2007. However, transactions and processes reviewed were not limited by the audit period.
Overall Conclusion

Of the three recommendations in the report, we determined that all three were partially implemented. However, the following risks are still present.

A. Without estimated response times, there is increased risk that the recovery teams will be delayed, which in turn lengthens the service interruptions for the User Community. The length of the service interruptions also affects how the User Community will carry out their continuity of operations plans. Users deserve to know what level of service to expect from BTS for a normal, critical, or catastrophic failure.

B. The department's plan to provide mandated and essential services is dependent upon when their applications and other support elements are restored. Departments risk not meeting mandates to provide critical services to the citizens if applications essential to their function cannot rely on recovery times estimated by BTS.

C. The cost estimates for the Disaster Recovery Plan need to be kept current to be useful. The cost estimates should be updated for major changes in the IT Environment, such as adding the Emergency Response Building facility or outsourcing the mainframe system to Verizon.

We commend management for their effort to implement our recommendations and continue to encourage management to fully implement the recommendations.

Background

The County previously has never had a formal Business Continuity or Disaster Recovery Plan relative to Information Technology (IT). The concept of the Business Continuity plan with Disaster Recovery and Operational Redundancy was developed under ITIL methodology. The County has adopted Information Technology Infrastructure Library (ITIL) methodology to deliver a framework of best practice approaches that can help align IT with business requirements, improve service quality, and lower the long-term cost of IT service provisions. Originally developed by the British government in the late 1980s, today ITIL is the world's most widely accepted approach to IT Service Management.

In the 2005 IT Strategic Plan, Business Continuity Planning was identified as a priority. A goal was set for “Operational redundancy for ‘mission critical’ systems; and a Disaster Recovery Plan will be developed, implemented, and tested.” CIBER Inc. (CIBER) was hired to assist in the Business Impact Analysis and to develop the initial Disaster Recovery Plan. CIBER completed a draft plan in June of 2005; the plan remained idle until IT created the position of Service Continuity Manager who took over responsibility for evaluating the plan in February of 2006. Its focus was to build a recovery plan so they could restore critical applications utilizing SunGard recovery services. The plan helped to identify multiple vulnerabilities in our operating
environment, equipment, and procedures. IT has addressed many of them already and continues to look for improvement. The hardening of the data center infrastructure (power and cooling), and much improved handling of our off-site tape storage are just a few of the items that were corrected. The Disaster Recovery Plan was developed without the benefit of a Business Continuity Plan.

In the 2006 IT Strategic Plan, Business Continuity was a major initiative to “develop and implement a Business Continuity and Disaster Recovery Plan.” The Business Continuity plan has not yet been completed. IT contracted with SunGard Recovery Services to provide the equipment necessary to restore several of our critical applications and to assist us with developing a recovery team and test plan. In November of 2006, the team conducted a tabletop exercise in preparation for a March 2007 test in Carlstadt, New Jersey.

In the 2007 IT Strategic Plan, IT considered participating with St. Petersburg College (SPC) in the development of a Business Continuity offering they are preparing. An initial test of the Disaster Recovery Plan was conducted in March 2007. A second test was conducted at the remote site in November 2007 using alternate team members. A third test was conducted at the remote facility in May 2008.

The Disaster Recovery Plan’s only exposure is the computer center. According to the Plan, “The loss of the Data Center located in the basement of the Courthouse provides the greatest single risk in terms of quantity of high priorities services.” The term “loss of the Data Center” relates to equipment that IT is responsible for in the basement of 315 Court Street. This did not include equipment managed and maintained by the Tax Collector, Property Appraiser, Clerk, or Information Systems. The Plan is only addressing the loss of the computer center, and assumes that “everything” in the County, other than the computer center, is 100% functional and fully staffed.

The Plan states, “While this initial effort is a critical first step towards developing a holistic plan for Disaster Recovery, there is much work still to do.”

While IT is enlarging its Disaster Recovery Plan and developing a Business Continuity Plan, all the areas that rely on information services should also be planning how they will continue operations. All the County Departments and Elected Officials developing Business Continuity Plans should address how they will handle interruptions of information services. The IT Business Continuity Plan will need to work in conjunction with the plans of all other County Department and Elected Officials to be effective.

If a County Department develops a Business Continuity Plan that relies on IT services, they should communicate these expectations and not simply assume it can be done. If your Business Continuity Plan contemplates relocating a hundred employees to another office location because of a flood or fire and they expect IT to have all their computers, printers and servers working within 48 hours, then it would be imperative to know if IT can really provide such support. Information Services need to be integrated into each area’s Business Continuity Plans to ensure the plans are realistic.
1. No Response Times For Service Levels Are Identified.

Service Levels that address action and time responses are not developed for the plan. The Disaster Recovery Plan has the roles and responsibilities set out, but no response times. The lack of response times impacts all the parties responsible for responding to the disaster or affected by the service interruption. Those areas that have no IT service will need to answer to citizens when they can expect to return to complete their business with the County.

The Disaster Recovery Plan has three different disaster levels as described in the policy.

- Disaster Level 3

Normal Impact(s)/Outage Situation(s) Affecting Daily Pinellas County Government IT Operations. Initial Trouble/Problem Reports are referred to the IT Help Desk; IT Help Desk Makes Referral to Appropriate Party for Resolution and Closure; Unresolved, Referred Problems are Escalated to Higher Levels of Management.

- Examples of Normal Impact(s)/Outage Situation(s):
  - Application failure
  - Server failure
  - Network failure
  - Viruses
Disaster Level 2

**Critical Impact(s)/Outage Situation(s) Affecting Daily Pinellas County Government IT Operations.** IT Unresolved Problems/Events of Critical Scope and/or Impact to Pinellas County Government IT are assessed by the Pinellas County Government IT Director for potential IT Disaster Declaration.

- Examples of Critical Impact(s)/Outage Situations:
  - Unresolved problems affecting critically important systems and/or technology environments for predetermined periods of time.
  - Unavailability of key staff for longer than a predetermined period of time.
  - Building evacuations.

Disaster Level 1

**Catastrophic Impact(s)/Outage Situation(s) Affecting Daily Pinellas County Government IT Operations.** Unresolved Problems/Events of Widespread Scope and/or Impact to Pinellas County Government are assessed by either the IT Director and/or the Pinellas County Government Chief Executive Officer.

- Examples of Catastrophic Impact(s)/Outage Situations:
  - Physical damage to the Computer Room.
  - Physical damage to Critical Equipment within the Computer Room.
  - Failure of the UPS and Generator.
  - Widespread impact to critically important systems and/or technology environments and/or their users.

The Disaster Recovery Plan responsibilities are split between three teams: Pinellas County Government Disaster Recovery Executive Team (DRE Team), Pinellas County Government IT Disaster Recovery Coordination Team (DRC Team), and Pinellas County Government Disaster Recovery User Liaison Team (DRUL Team). The Disaster Recovery Manager has the responsibility to notify the teams in case of a disaster. The Disaster Recovery Plan, however, does not refer to any of the three different levels of disasters. There is no service level set for knowing which team(s), Executive, Coordination or User Liaison, to notify, or the expected time frame. It follows that the User Community would also have no idea when they would be notified in case of a disaster.

A framework for IT governance and control, Control Objectives for Information and Related Technology (COBIT), was used as a standard to perform the audit. COBIT standards suggest that response and recovery requirement be done in time period tiers, and that recovery be in
line with prioritized business needs. The various disaster levels should have corresponding response service levels in different tiers corresponding to critical business operational periods.

Service interruptions are initially handled through the IT Customer Support Center (CSC) using the Computer Associates "Service Desk" program. The Customer Support Center prioritizes the incident. The Support Center Call notification Communication Plan and notification are based on incident Priority levels of 1, 2, or 3, and not Disaster Levels. The Customer Support Center handles the Incident Management responsibility that falls under IT Service, Service Management.

The Disaster Recovery Plan does not have service levels defined in the same manner as Incident Management. Incident Management uses the Incident Management Prioritization Model to prioritize incidents and set target response, recovery and resolution times. The response time is the acknowledgement to the customer. The recovery time refers to when someone will be actively working on the problem. The target resolution time refers to when the service is restored. The service level time frame includes the response, recovery, and resolution times. The Disaster Recovery Plan only sets all recovery times as simultaneously within 24 to 48 hours, but suggests setting priorities and resolution times. See Appendix A for Section 4, Recovery Measurement of the Disaster Recovery Plan, for more detail.

The Disaster Recovery Plan has service responsibilities assigned, but they are not associated with any service level time frame. The teams and designated positions, such as the Disaster Recovery Manager, have specific responsibilities. In the Disaster Recovery Plan, the Disaster Recovery Manager has the responsibility for team notification, but no specifics on time. An example of a service level response might be that the Disaster Recovery Manager, within one hour of notification of a Level 2 Critical Impact disaster, will in turn notify the Government Disaster Recovery Executive Team. In this example, the DRE Team can expect to be notified within one hour of when a critical impact disaster has occurred.

IT has contracted with SunGard to provide disaster recovery services and facilities for our Disaster Recovery Plan. SunGard reviewed our completed plan and provided us a Post Project Report dated March 30, 2007, which included their observations. SunGard observed that, “The user community isn’t fully aware of the level of service to expect from the IT group following a disaster.” They recommended that a disaster service level agreement be developed to communicate recovery time.

The Disaster Recovery Plan needs to set out response times for all levels of service interruptions. The IT Customers using those services in serving the citizens are certainly entitled to some response. The User Community should understand how and when they will be contacted in case of a disaster.

Recommendation:

Management establish service levels for response times for all parties affected by a disaster in the computer center. The Disaster Recovery Plan needs to establish target response times
that correspond with individual and team responsibilities. The response times should support the user's need in terms of critical business operational periods.

Management Response:

We concur. The Disaster Level for this Plan was focused on a catastrophic event, the total loss of the data center. With that in mind, the Recovery Time Objective (RTO) is 72 hours, (3-5 days) for "critical" applications and not 24-48 hours as stated in the audit. The Recovery Point Objective (RPO) is the point in time to which systems and data must be recovered after an outage needs to be determined by the individual agencies. Our Service Manager is working with our customers to develop Service Levels. We need to establish underpinning contracts with third parties responsible for supporting the infrastructure and equipment. The Disaster Levels in the Plan coincide with our Levels of priority at the Customer Support Center.

Status:

Partially Implemented.

BTS has set service for a catastrophic event at an estimated 3-7 days under the contract with SunGard. BTS is currently in the process of modifying the contract with SunGard to provide recovery services for the mainframe and network. The service levels for response time still need to be established for both the SunGuard and Emergency Response Building for each level of failure in the Disaster Recovery Plan. The teams responsible for responding to normal, critical, and catastrophic levels of service interruptions will need to determine the cause to estimate how long recovery is expected to take. Without estimated response times, there is increased risk that the recovery teams will be delayed, which in turn lengthens the service interruptions for the User Community. The length of the service interruptions also affects how the User Community will carry out their continuity of operations plans. Users deserve to know what level of service to expect from BTS for a normal, critical, or catastrophic failure.

2. Recovery Time Objectives Are Not Estimated For Disaster Levels.

The Disaster Recovery Plan outlines the approach to setting recovery times, but no time estimates have been set. The effect of not setting time objectives in the plan prevents communication to users as to when IT service would be restored. COBIT standards suggest that response and recovery requirements be done in tiers (time periods) and critical business operational periods (business hours/weekends).

The User Community wants to know how long until they can use their application to serve the citizens. Of course, the users will also want to know if there will be any limitation to the service, such as slow response time. The Disaster Recovery Plan makes an assumption that all network connectivity is not affected by the disaster. The users need to understand the extent of the service level outage to manage their own business continuity plan. Since most governmental functions operate from one or more information systems, the recovery time and
any capacity limitations are parameters that affect management's decisions on implementing business continuity plans.

The Disaster Recovery Plan defines recovery time objectives as the period of time within which systems, applications or functions must be recovered after an outage. The plan breaks recovery time into two parts, a base recovery time and an operations recovery time. The base recovery time is simply how long it will take to have the computer center in production at the alternate site, Philadelphia, Pennsylvania. The operations recovery time is how long it takes to get the user's application information system running. The recovery time objective is the period of time needed to restore user's application systems as illustrated below.

The Disaster Recovery Plan, however, does not have an estimated recovery time objective set because there is no estimate for how long it will take to get the alternate SunGard computer center in Philadelphia running. Base Recovery Time Frames by "operating system" are as follows: Currently the Base Recovery Time Frames are not known and will be dependent on the Hotsite strategy. Operation Recovery Time Frames by “application” are as follows:

Currently all critical applications would be recovered simultaneously within 24 to 48 hours. The recovery time objective should be set to correspond with the
various levels of disasters. For example, there should be a recovery time objective for a complete loss of the data center, a catastrophic event.

The Disaster Recovery Plan addresses disasters as, "In general terms, a disaster, or emergency event is any situation that leaves the business in a less than fully productive state for a period of time that would affect critical processing capabilities. This means that if an organization suffers a loss of data, loss of integrity or reliability in IT processing, or loss in the means by which data is communicated, manipulated, or presented for use, a 'disaster' has occurred. Disaster conditions can occur at a variety of levels ranging from the 'very minor' isolated hardware outage to the complete loss of the Data Center." The plan goes on to say, "Finally, it is important to note that a disaster need not be catastrophic in nature for a business to be affected. As long as the result of the event is an unacceptable interruption of normal business operations, the event can be classified as a 'disaster'.”

The following events clearly define a Pinellas County Government IT "Disaster":

- Inability of the Pinellas County Government Computer Center to process or support critically important business processes for more than <= 12 ?? ?? >> hours.
- Catastrophic damage to the Pinellas County Government IT Computer Center.
- Any event defined categorically as a "disaster" by the Disaster Recovery Manager, IT Director, or Pinellas County Government County Administrator.

As noted previously, the Disaster Recovery Plan has three disaster levels; normal, critical and catastrophic.

Although the Disaster Recovery Plan disaster defines a "disaster or emergency" in terms of service interruptions to users, the impact goes beyond the users to the citizens they serve. This is especially important when those users are responsible for emergency services. The Comprehensive Emergency Management Plan 2006 (CEMP) that lists the supporting plans does not include the Disaster Recovery Plan. The CEMP also has a section on County departments and responsibilities. Information Technology is shown to have the Response Function "Maintain Computer Network" and the Recovery Function "Restore Computer Network." The Disaster Recovery Plan is a component of the IT Business Continuity Plan. The Business Continuity Plan is currently planned for in the 2007 IT Strategic Plan. The IT Disaster Recovery Plan's recovery time objective is the key to when users can again provide services to the citizens.

As previously mentioned SunGard reviewed the Disaster Recovery Plan and provided us a report, which included their observations. SunGard observed that The Information Technology (IT) Recovery Plan is not fully integrated with Continuity of Operations (COOP) planning. They recommended that requirements and capabilities are clearly established for the overall Pinellas County response and recovery planning efforts. SunGard also observed that the current Plan does not include well-defined disaster declaration criteria. They recommended that IT and Business Continuity planners work together to define the appropriate triggers requiring disaster declaration and activation of the Recovery Plan.
The users need to know the estimated length of the service interruption to manage their own business continuity plan. The Disaster Recovery Plan makes an assumption that all network connectivity is not affected by the disaster. Since most governmental functions operate from one or more information systems, the users will be serving the citizen when the computer center is restored along with network connectivity to the their systems. The recovery point objective will affect management's decisions on implementing business continuity plans.

Recommendation:

Management establish recovery times that communicate to the users the expected availability of the information systems.

Management Response:

We partially concur. The recovery times have been communicated to our users and they understand their recovery times will differ based on the type of disaster, critical of the application and system. Several applications cannot tolerate 1 or 2 hours of down time in a “normal” day. These applications will be considered for the hot site. If the event were regional, they would be okay being down for a few days. It all depends on the type of disaster we have at hand. We would not have any idea of how long a service will be out until the situation is fully assessed. If the computer room is under six feet of water . . . we will have a pretty good idea that the systems will be down for 3 – 5 days; however, if the problem is a failed server, this may be only several hours.

Status:

Partially Implemented.

Some significant events have occurred that affect the disaster plan recovery times. Emergency Management, in revising their Continuity of Operations plans, has increased their expectation of BTS to provide services. BTS has installed servers at the Emergency Response Building to support applications that had originally been contracted with SunGard for recovery. The necessary County Services identified by Emergency Management need to correspond to what BTS can restore in their Disaster Recovery Plan. The recovery times establish when the basic computer infrastructure is in place to allow for continued operation of necessary County services. The department must identify the applications and other support elements necessary to conduct mandated/critical services. The department's plan to provide mandated and essential services is dependent upon when their applications and other support elements are restored. Departments risk not meeting mandates to provide critical services to the citizens if applications essential to their function cannot rely on recovery times estimated by BTS.
3. No Cost Estimates For Activating A Remote Computer Facility Has Been Included As A Factor.

The Disaster Recovery Plan provides an option to activate the remote computer center, but this could cost over a million dollars. Management needs to consider costs when deciding to activate the remote computer facility.

At this point in the Disaster Recovery Plan, service has been interrupted by a disaster to the computer center and an assessment of the damage has been made. Management will be deciding how to restore IT services. Management will consider repair and replacement scenarios for facilities and equipment for which time and cost will be important factors. The Disaster Recovery Plan should also provide time and cost estimates for management to consider. The time estimates would include the recovery time objectives previously discussed.

Although there are no cost projections currently in the Disaster Recovery Plan, IT was developing costs for their business case to justify a hot site. We used the IT business case cost as a basis for our estimate for SunGard and Personnel costs. The activation costs for a remote computer facility for 30 days should be at least $1 million; considering SunGard facility costs of $910,000 and personnel cost of $82,650, which does not include any overtime. The activation costs for a remote computer facility for 14 days should be at least $500,000, which does not include any overtime.

The personnel costs need to consider overtime costs. The IT personnel cost estimate simply assumed that ten employees would be sent to the warm site in Philadelphia, work no overtime, and return after 30 days. The simplified personnel cost estimate needs to be expanded to at least include a Fair Labor Standard Act (FLSA) workweek schedule. The FLSA requires that a fixed workweek or a work cycle (28-day work cycle) be established in order to determine overtime pay for classified employees. The most important aspects that relate to the Disaster Recovery Plan have to do with scheduling 10 correctly trained persons to operate the warm site for 30 days. The warm site activation requires initially a large personnel effort which will be followed by operations on a 24/7 basis requiring various shifts. Planning shift schedules would set out hours worked, overtime and compensatory time for the initial activation and for ongoing maintenance. Consideration should also be given to a shift change every two weeks to reduce overtime and increase employee morale.

The only mention of cost in the Disaster Recovery Plan is in regard to the risk analysis, page 17, "A Risk Analysis is conducted to help managers strike an economic balance between the impact of risks and the cost of protective measures." This also applies to decisions for the different courses of action in the Disaster Recovery Plan. When management is asked to decide whether to activate the warm site, they should weigh the costs of this course of action.

Recommendation:

Management include cost estimates for decision-making. The cost projections should include all costs to establish and operate the remote facility, including facility fees, shipping charges
and personnel costs. Personnel costs should take into account overtime costs necessary for the initial activation and for ongoing 24/7 staffing.

Management Response:

We concur. At the time the plan was developed, costs were not a factor. The current plan is to have between 8 and 10 staff members participate in the offsite recovery effort. We did not account for staff that would be needed here to "rebuild" the data center. Most of the Business Technology Services (BTS) staff are classified employees and would be subject to FLSA overtime rules.

Here are the costs to declare a disaster under the current SunGard plan:

- Declaration – Day one, $62,500.
- Day two through thirty equals $26,750 per day.
- The 31st day and beyond equals $35,500 per day.
- Pinellas County Staff, (10 classified), transportation, accommodations, meals, and overtime for 30 days, $201,650.

Status:

Partially Implemented.

The cost estimates for the Disaster Recovery Plan need to be kept current to be useful. The cost estimates should be updated for major changes in the IT Environment, such as adding the Emergency Response Building facility or outsourcing the mainframe system to Verizon.
Appendix A
Information Technology Disaster Recovery Plan Version 3.6

4 Pinellas County Government – Recovery Measurements

4.1 Analysis and Prioritization of Applications

The following table lists the Recovery Priority of Pinellas County Government Applications, as developed from the analysis of data collected in the Pinellas County Government Business Impact Analysis February 2005.

<table>
<thead>
<tr>
<th>(Recovery) Prioritization of Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical Applications will be reviewed regularly</td>
</tr>
</tbody>
</table>

- CJIS
- Internet Access
- Email / Exchange and all supporting infrastructure
- VPN Access
- Oracle Financials
- Oracle Purchasing
- Main Frame access / Rumba
- Antivirus - Enterprise
- Permits Plus
- Netware – File Print for all campus are BCC Depts.
- GIS Server – (Map Guide / EMA Supported Application)
- Pinellas County Web Site
- Tivoli – Enterprise Backup Services
- Animal Services
- General Services Imaging
- OMB Applications
- Medical Examiner
4.2 Recovery Point Time Objective (RPO)

**RECOVERY POINT OBJECTIVE (RPO):** The point in time to which systems and data must be recovered after an outage as determined by the business unit.

4.3 Recovery Time Objective (RTO)

**RECOVERY TIME OBJECTIVE (RTO):** The period of time within which systems, applications, or functions must be recovered after an outage (e.g., one business day). RTOs are often used as the basis for the development of recovery strategies, and as a determinant as to whether or not to implement the recovery strategies during a disaster situation.

“Recovery Time Objective” is defined as that time measured from Disaster Declaration, through recovery, until the start of “in production” IT Operations in the alternate processing site. “Recovery Time Objective” equals “Base Recovery Time Frame” plus “Operations Recovery Time Frame.”

4.4 Base Recovery Time Frame

“*Base Recovery Time Frame*” is defined as that time measured from Disaster Declaration, through Installation/Integration and Verification of Operating System software on target hardware at the specified alternate processing site.

4.4.1 Base Recovery Time Frames by ‘operating system’ are as follows:

<table>
<thead>
<tr>
<th>Computer/Operating System</th>
<th>Base Recovery Time Frame (Hours)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Currently the Base Recovery Timeframes are not known, and will be dependent on the Hot site strategy</td>
</tr>
<tr>
<td>MVS</td>
<td></td>
</tr>
<tr>
<td>VM</td>
<td></td>
</tr>
<tr>
<td>Intel Windows</td>
<td></td>
</tr>
<tr>
<td>Novell</td>
<td></td>
</tr>
<tr>
<td>Linux</td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td></td>
</tr>
<tr>
<td>CICS</td>
<td></td>
</tr>
<tr>
<td>RISC/AIX</td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td></td>
</tr>
</tbody>
</table>
4.5 Operations Recovery Time Frame

"Operations Recovery Time Frame" is defined as that time measured from the Verification of Operating System software through Installation/Integration and Verification of Application Software and User-Level Access to Target Applications at the specified alternate-processing/recovery site.

REFERENCE THE RECOVERY PROCEDURES

4.5.1 Operations Recovery Time Frames by 'application' are as follows:

<table>
<thead>
<tr>
<th>Application System</th>
<th>Operations Recovery Time Frame (Hours)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM Z800</td>
<td>Currently all applications would be recovered simultaneously within 24 to 48 hours</td>
</tr>
<tr>
<td>Delinquent Tax-Real Estate.</td>
<td></td>
</tr>
<tr>
<td>Child Support Inquiry.</td>
<td></td>
</tr>
<tr>
<td>Warrants (Inquiry and Maintenance).</td>
<td></td>
</tr>
<tr>
<td>Animal Control System.</td>
<td></td>
</tr>
<tr>
<td>Vehicle Registration Inquiry.</td>
<td></td>
</tr>
<tr>
<td>Master Appraisal Records.</td>
<td></td>
</tr>
<tr>
<td>Consumer Affairs Complaint System.</td>
<td></td>
</tr>
<tr>
<td>Subdivision Search.</td>
<td></td>
</tr>
<tr>
<td>Juvenile Information System.</td>
<td></td>
</tr>
<tr>
<td>Civil/Small Claims.</td>
<td></td>
</tr>
<tr>
<td>Law Enforcement Name Index.</td>
<td></td>
</tr>
<tr>
<td>Tax Rolls-Name Index.</td>
<td></td>
</tr>
<tr>
<td>Probate Court.</td>
<td>(Pinellas County needs to prioritize all applications in order to have a planned recovery process)</td>
</tr>
<tr>
<td>Parking Ticket Inquiry.</td>
<td></td>
</tr>
<tr>
<td>Tax Rolls-Real Estate/Personal Property.</td>
<td></td>
</tr>
<tr>
<td>Domestic/Repeat Violence-Update.</td>
<td></td>
</tr>
<tr>
<td>Delinquent Tax-Personal Property.</td>
<td></td>
</tr>
<tr>
<td>Florida Bar Attorney File.</td>
<td></td>
</tr>
<tr>
<td>Warrants (Enter New Warrants).</td>
<td></td>
</tr>
<tr>
<td>Official Records Fictitious Names.</td>
<td></td>
</tr>
<tr>
<td>Update Stolen Vehicle Code.</td>
<td></td>
</tr>
<tr>
<td>Geographic Address Lookup.</td>
<td></td>
</tr>
<tr>
<td>Records &amp; ID System.</td>
<td></td>
</tr>
<tr>
<td>Real Estate Search by Parcel Number.</td>
<td></td>
</tr>
<tr>
<td>Real Estate Search by Owner.</td>
<td></td>
</tr>
<tr>
<td>Supervisor of Elections.</td>
<td></td>
</tr>
<tr>
<td>Marriage License Inquiry.</td>
<td></td>
</tr>
<tr>
<td>Justice Information.</td>
<td></td>
</tr>
<tr>
<td>Official Records Plats/Restrictions.</td>
<td></td>
</tr>
<tr>
<td>Traffic Information.</td>
<td></td>
</tr>
<tr>
<td>Domestic/Repeat Violence – Add.</td>
<td></td>
</tr>
<tr>
<td>Bankruptcy System.</td>
<td></td>
</tr>
<tr>
<td>Web Sphere.</td>
<td></td>
</tr>
<tr>
<td>Several Oracle databases.</td>
<td></td>
</tr>
</tbody>
</table>

Example:
Priority 1 = 24-48 hours
Priority 2 = 48-72 hours
Priority 3 = 72-120 hours
### AIX

<table>
<thead>
<tr>
<th>Application System</th>
<th>Operations Recovery Time Frame (Hours)</th>
</tr>
</thead>
<tbody>
<tr>
<td>APPX.</td>
<td>Currently all applications would be recovered simultaneously within 24 to 48 hours</td>
</tr>
<tr>
<td>Oracle.</td>
<td>(Pinellas County needs to prioritize all applications in order to have a planned recovery process)</td>
</tr>
<tr>
<td>Clerk CWS.</td>
<td>Example: Prioritiy 1 = 24-48 hours</td>
</tr>
<tr>
<td>Development.</td>
<td>Priority 2 = 48-72 hours</td>
</tr>
<tr>
<td>Old Web Sphere.</td>
<td>Priority 3 = 72-120 hours</td>
</tr>
<tr>
<td>BCC CWS.</td>
<td></td>
</tr>
<tr>
<td>Clerk Child Support.</td>
<td></td>
</tr>
<tr>
<td>GIS.</td>
<td></td>
</tr>
<tr>
<td>Oracle Application Server.</td>
<td></td>
</tr>
<tr>
<td>Oracle Financials.</td>
<td></td>
</tr>
<tr>
<td>GIS Database.</td>
<td></td>
</tr>
<tr>
<td>Vision.</td>
<td></td>
</tr>
<tr>
<td>GEMS.</td>
<td></td>
</tr>
<tr>
<td>Oracle Medical Examiner.</td>
<td></td>
</tr>
<tr>
<td>Project Management</td>
<td></td>
</tr>
<tr>
<td>Maximo</td>
<td></td>
</tr>
<tr>
<td>Eops</td>
<td></td>
</tr>
<tr>
<td>Lims</td>
<td></td>
</tr>
</tbody>
</table>

### INTEL

<table>
<thead>
<tr>
<th>Application System</th>
<th>Operations Recovery Time Frame (Hours)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Currently all applications would be recovered simultaneously within 24 to hours</td>
<td></td>
</tr>
</tbody>
</table>

Pinellas County needs to prioritize all applications in order to have a planned recovery process |

Example: Prioritiy 1 = 24-48 hours |
Priority 2 = 48-72 hours |
Priority 3 = 72-120 hours |
DIVISION OF INSPECTOR GENERAL

KEN BURKE, CPA
CLERK OF THE CIRCUIT COURT
PINELLAS COUNTY, FLORIDA

Write: Fraud Hotline
      Public Integrity Unit
      Division of Inspector General
      400 Cleveland St., 4th floor
      Clearwater, FL 33755-4041

Phone: (727) 453-3728
      Fax: (727) 464-8386

E-Mail: fraudhotline@pinellascounty.org
Internet: www.mypinellasclerk.org

Accredited Office of Inspector General
by the Commission for Florida Law Enforcement Accreditation