City of Gainesville ***Inter-Office Communication***

April 3, 2012

TO: Audit, Finance and Legislative Committee
Mayor Craig Lowe, Chair
Mayor-Commissioner Pro Tem Thomas Hawkins, Member

FROM: Brent Godshalk, City Auditor

SUBJECT: Review of GRU Information Technology Disaster Recovery

Recommendation

The Audit, Finance and Legislative Committee recommend that the City Commission:

1) Accept the City Auditor's report and the response from the General Manager for Utilities, and

2) Instruct the City Auditor to conduct a follow-up review on recommendations made and report the results to the Audit, Finance and Legislative Committee.

Explanation

In accordance with our Annual Audit Plan, the City Auditor's Office has completed a Review of GRU Information Technology (IT) Disaster Recovery. The primary objective of our audit was to evaluate the adequacy of GRU policies, procedures and plans related to information technology disaster recovery and data backup. During our review, we interviewed key personnel, reviewed procedures manuals, inspected the data center and evaluated management controls.

Based on the results of our review, we believe the GRU IT Disaster Recovery process has strong internal controls in place and uses sound approaches to help ensure that GRU will be able to recover data and resume operations timely in the event of a disaster. We do have three recommendations regarding classroom or functional exercises, improved documentation regarding visitor activity in data centers and timely completion of incomplete Data Recovery Plan elements which we believe will help to strengthen management controls in this area.

We request that the Committee recommend the City Commission accept our report and the General Manager's response. Also, in accordance with City Commission Resolution 970187, Section 10, Responsibilities for Follow-up on Audits, we request that the Committee recommend the City Commission instruct the City Auditor to conduct a follow-up review on recommendations made and report the results to the Audit, Finance and Legislative Committee.

City of Gainesville

Inter-Office Communication

February 29, 2012

TO: Bob Hunzinger, General Manager for Utilities

FROM: Brent Godshalk, City Auditor

SUBJECT: Review of GRU Information Technology Disaster Plan

In accordance with our Annual Audit Plan, the City Auditor's Office has completed a Review of GRU Information Technology (IT) Disaster Recovery. The primary objective of our audit was to evaluate the adequacy of GRU policies, procedures and plans related to information technology disaster recovery and data backup. During our review, we interviewed key personnel, reviewed procedures manuals, inspected the data center and evaluated management controls.

Based on the results of our review, we believe the GRU IT Disaster Recovery process has strong internal controls in place and uses sound approaches to help ensure that GRU will be able to recover data and resume operations timely in the event of a disaster. The attached report provides three recommendations regarding classroom or functional exercises, improved documentation regarding visitor activity in data centers and timely completion of incomplete Data Recovery Plan elements which we believe will help to strengthen management controls in this area.

Our recommendations for improvement have been reviewed with Jennifer Hunt, Chief Financial Officer and David Darus, IT Infrastructure and Administration Manager during an exit conference on February 28th. I would like to acknowledge their professional courtesy and cooperation during our review.

Please review the attached written report, which documents our audit recommendations and provide a written response within 30 days. Our report, including the management responses, will then be submitted to the City Commission's Audit, Finance and Legislative Committee for review and approval. The next meeting is currently scheduled for April 3, 2012. Until that time, this draft report and your draft response are exempt from Florida's public records law.

Thank you to you and your staff for making this a productive process. Feel free to call me if you have any questions.

cc: Jennifer Hunt, Chief Financial Officer
David Darus, IT Infrastructure and Administration Manager

OBJECTIVES, SCOPE AND METHODOLOGY

In accordance with our Annual Audit Plan, the City Auditor's Office completed a Review of GRU Information Technology (IT) Disaster Recovery. The primary objective of this audit was to evaluate the adequacy of GRU policies, procedures and plans related to information technology disaster recovery and data backup. During our review, we interviewed key personnel, reviewed procedures manuals, inspected the data center and evaluated management controls. Our procedures included interviewing key personnel, observing operations, reviewing benchmark data and recommendations developed by the U.S. Department of Commerce National Institute of Standards and Technology, evaluating management controls and reviewing trends in disaster recovery. The scope of our review was the Data Recovery Plan (DRP) for March 2011.

As for all of our audits, 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.

Based on the results of our review, we believe the GRU IT Disaster Recovery process has strong internal controls in place and uses sound approaches to help ensure that GRU will be able to recover data and resume operations timely in the event of a disaster. However, opportunities exist to strengthen the GRU IT Disaster Recovery process through classroom or functional exercises, improved documentation regarding visitor activity in data centers and timely completion of incomplete Data Recovery Plan elements. Each of our recommendations has been discussed with management. These recommendations, as well as management's written response, can be found in the following sections of this report.

BACKGROUND INFORMATION

The National Institute of Standards and Technology (NIST) is an agency within the U.S. Department of Commerce that makes measurements and sets standards as needed by industry or government programs. This includes disaster recovery plans. NIST states an effective disaster recovery plan should include a combination of preventive, detective and corrective measures to ensure a smooth continuity of business operations in the event of a disruption or disaster. The plan should address the basic stages of emergency reaction including emergency response, backup operations, and recovery operations.

Types of Disaster

An IT business unit is exposed to potential threats resulting in lost data that can be minimized or eliminated through technical, management or operational solutions. There are three types of threats to an IT system including:

- Natural – Includes hurricanes, tornadoes, floods and fire.
- Human – Encompass operator error, sabotage, implant of malicious code and terrorist attacks.
- Environmental – Includes equipment failure, power failure and software error.

The GRU DRP is designed for any natural, human or environmental event that may occur. A data recovery procedures manual may be accessed through GRUITpedia and provides staff with information regarding data centers, databases, hardware, servers and systems. In addition, it includes a GRU self-training section for employees to review steps that should be taken in the event of an emergency. The

DRP also includes maintenance schedules, checklists for task to perform daily, weekly and monthly and an assignment schedule for the current year.

Disaster Recovery Plan

NIST suggests that a DRP include:

- A defined purpose.
- Applicability which documents the organization impacted by the IT contingency plan.
- A scope that identifies the target and addresses assumptions in the plan and the key personnel available during an emergency.

A disaster recovery plan defines roles and responsibilities, resource requirements, training requirements, exercise and testing schedules, plan maintenance schedule and frequency of backups and storage of backup media.

GRU IT has developed a system support mission which outlines GRU IT responsibilities and staffing including hardware, operating systems, development tools, application support software and technical expertise. It also identifies staff positions responsible for all aspects of the GRU computing infrastructure. The plan also includes eight IT System support principles ranging from building redundant, highly available, durable and recoverable systems, secure systems, well-documented systems and striving for self-sufficiency without requiring vendor and consultant support.

In addition to the comprehensive guide there is a “GRU IT Hurricane Plan” which provides specific procedures to follow for a natural event that is likely to affect the area. The “GRU IT Hurricane Plan” provides contacts, a preparation checklist, a user support plan and an infrastructure and programming support plan.

Alternate Site Locations

NIST also suggests alternate sites for backup to recovery. Factors to consider when determining alternate site locations include:

- Geographic – distance from the organization and the probability that the same disaster would occur in the area.
- Accessibility – length of time to retrieve the data from storage and the storage facilities operating hours.
- Security – security capabilities of the storage facility.
- Environment – structural and environmental conditions of the storage facility.
- Cost - cost of shipping, operational fees and disaster response.

GRU has done this with a dedicated site within GRU owned properties. GRU uses its own facilities to maintain backup. This ensures the accessibility, security, environment and cost issues. Geographically there is a weakness with this approach. Since a natural disaster could impact both the Data Center and secondary location, there is a risk to maintaining a secondary backup a few miles apart. As we have seen with other disasters in which entire cities can be severely devastated by a natural disaster, the secondary location could be affected as much as the primary location. However, GRU has accepted this risk since the costs outweighs the possibility of a catastrophic disaster effecting both locations.

Preventive Controls

Preventive controls lessen the potential for data loss. GRU has several preventive controls that NIST suggests including, but not limited to:

- Generators that provide long term backup power.
- Air conditioning capacity to permit failure of certain components.
- Fire suppression system.
- Fire and smoke detectors.
- Frequent, scheduled backups.

GRU IT requires staff to annually review the operation of preventive controls, including whom to notify and how to activate equipment if an emergency or potential equipment failure should occur within the Data Center.

Plan Maintenance

NIST advocates a strict control of the recovery plan document to ensure that each employee is working from the current approved copy in the event of a disaster. GRU eliminates the need to ensure strict control of the DRP. The current copy of the DRP is placed on a USB thumb drive maintained in a vault. The thumb drive is secured by the IT Infrastructure and Administration Manager and Lead IT Infrastructure Designer and Administrator. The current copy is maintained online within GRU's GRUITpedia which enables staff to access and review the most current plan.

The DRP is updated on an on-going basis. If GRU has new or updated software or developments, then these are included in the plan once they become operational. Changes to the DRP can only be made by authorized staff.

According to NIST, the DRP should be formatted to provide quick and clear direction in the event that personnel unfamiliar with the plan or system are called to perform recovery operations. GRU does have supporting information that provides background information that includes:

- System description includes the IT system architecture, location and technical considerations.
- Line of succession identifying personnel responsible to assume authority for executing the plan.
- Responsibilities including the overall structure of the contingency team and hierarchy.

Recovery Procedures

GRU has established four tiers in order of mission critical for implementation of the DRP. A damage assessment team will assess damage and activate the plan including all recovery phases. The four tiers, from most critical to least critical, include:

Tier 1 – Infrastructure. Ensuring basic support services are established.
Tier 2 – Production-Business Critical. Applications critical to GRU affecting a large number of users.
Tier 3 – Production-Departmental. Applications affecting fewer users and less critical than Tier 2.
Tier 4 – Development and Standby. Classified as the least critical phases to recover.

GRU procedures include establishing a command center, including the equipment required to perform the task. There are step-by-step instructions for restoring the IT system and system components.

Typically, GRU activates a disaster recovery plan during a hurricane or tropical storm event. In 2004, staff was prepared to enact the disaster plan if necessary during the tropical storm events that affected Gainesville. Each time, the plan was not needed to be implemented. In 2009, the DRP was used successfully for a system-wide shutdown to install a new storage system.

GRU also performs monthly and quarterly maintenance testing. Maintenance testing is done to put updates or current fixes to ensure application continue to run effectively. The test teams will indicate the downtime expected, systems affected, note any change explanations and include management approval for change. Notes are made if unexpected events occur or if the procedures require changes for the future. These are reviewed by management and if necessary those changes may be included in the DRP.

ISSUE #1

Classroom or Functional Exercises Should Be Performed on a Test Basis

Discussion

NIST describes plan testing, training and exercises as a critical element of a viable contingency plan. By performing tests, plan deficiencies can be identified and addressed. Testing also helps evaluate the ability of the recovery staff to implement the plan quickly and effectively. To derive the most value from the test, a Disaster Plan Coordinator develops a test plan. The test plan should delineate a clear scope, scenarios and logistics. The scenario chosen may be a worst-case incident or one that is likely to occur. There are two basic formats for exercise: classroom and functional. The classroom exercise is considered very basic and the least costly to perform. This exercise involves talking through a scenario, with each staff relaying what their role is during the disaster. Functional exercises are more extensive and involve a fictional event through which the team can simulate the recovery.

GRU performs an annual training exercise for all IT staff responsible for data recovery with regard to security, safety, environmental, UPS, fire suppression and air conditioning within the Data Center. This includes talking through operating the fire suppression system, environmental monitoring, security issues and other critical issues. GRU also had a planned shutdown requiring the use of the DRP in order to upgrade new systems. The DRP was also in place for the series of hurricanes in 2004, however, GRU did not lose power or data that required the DRP to be fully activated.

GRU does not perform either a classroom or functional test plan in which a disaster is simulated. NIST states that a test plan should be designed to test selected elements against explicit test objectives and success criteria. The use of test objectives and success criteria enables management to assess the effectiveness of each plan element and the overall test plan to be assessed. Test plans should be designed to assess various components of GRU’s IT services if a total disaster occurs. This would allow GRU IT and departments to evaluate the overall level of disaster recovery readiness. It would enable GRU IT to evaluate annually concerns that may be addressed with all participants together. This would also enhance the data center training already performed by staff on an annual basis.

GRU has not performed this type of training because the time needed to prepare a simulation has not been available. Additionally, prior to the Eastside Operations Center, the primary data center at the GRU Administration Building did not provide sufficient room to perform such a test.

Conclusion

There is no classroom or functional testing performed to prepare staff for an emergency from start to conclusion. GRU increases the risk for a complete recovery in the event of a disruption or disaster without an active DRP exercise that includes all recovery staff and begins at the start of an emergency to determine where potential weaknesses may be in a total recovery.

Recommendation

GRU IT should at a minimum perform classroom testing with specific goals and objectives determined prior to the test that would simulate a potential real-life incident. This should be done annually, prior to hurricane season, which potentially offers the greatest concern for disruption or recovery of data. This type of exercise will enhance the evaluation of the disaster recovery test as well as allow for a meaningful update to the disaster recovery plan.

Management's Response

GRU IT will develop and conduct simulation training by 6/30/2013. In the FY12 hurricane season we will focus our efforts on utilizing the new EOC Data Center for production system by 7/31/2012. This work will enhance our disaster avoidance plan. The IT infrastructure staff has at least informal knowledge and training on disaster recovery thus the simulation training can wait until next hurricane season.

ISSUE #2

Improved Documentation of Visitor Activity in Data Centers

Discussion

We reviewed the data center procedures and performed a walk-through of the area to ensure:

- the center is restricted to authorized individuals,
- sensitive information is protected from environmental hazards,
- system backup and recovery procedures adequately protect against critical data loss,
- business continuity and disaster recovery is supported,
- sensitive equipment is protected against loss of power, fluctuations and inadequate maintenance operations, and
- policies and procedures adequately support the protection and efficient operation of GRU systems and data.

The data center houses computer equipment containing mission critical information systems and data essential to GRU operations. An electronic key card allows access into the data center. Access reports are generated, provided monthly and communicated to those managers responsible for governance of the process. Those who review the reports ensure only authorized personnel accessed the center during the previous month. If unauthorized staff entered the data center, follow up is done to determine if the employee's access authorization changed or if the electronic key card needs to be changed to deny access.

The primary data center at the time of our review was secured in the basement of the GRU Administration Building. Visitor access to the building is through a security guard and requires the visitor to identify the employee he or she is meeting. The visitor signs a log indicating the date, time and who will be visited. The GRU employee then meets the visitor to provide access beyond the lobby. During our visit of the data center, we observed this practice. Although the sign-in log indicates the individual visited GRU, it does not include or note that a "visitor" would be entering the data center. Therefore, those monitoring access will not know through data center access reports which visitors entered the data center.

Since the data center maintains all critical equipment and data, anyone entering the data center, even when escorted by staff, is potentially an individual that provides some security risk. The data center's electronic key card system prevents unauthorized individuals from entering the center; however, it does not provide a record of all employees or visitors who have entered the data center. An electronic security card exclusive to a GRU visitor to the data center would provide a method to monitor the day and time a visitor gained access. The card number could be noted next to the visitor's name in the employee log. When the visitor is escorted to the data center the electronic card key will note that a visitor entered on that day and time. This will also provide a measure of how many visitors access the data center and if these are authorized visitors.

The Eastside Operations Center (EOC) will become the primary data center during the summer of 2012 with the GRU Administration Building serving as the secondary backup data center. Enhanced security measures are scheduled to be in place at the EOC. Since the GRU Administration Building will serve as the primary backup, security procedures should be enhanced to better ensure only authorized staff and visitors have access to the center and such access is adequately documented and reviewed.

Conclusion

GRU uses a multiple layer exterior security system with camera coverage at the front entrance, security guards, and sign in procedures at the front entrance of the Administrative Building. The Data Center only has access by authorized employees through a key card system. Although this prevents anyone from entering, it does not provide a record of all individuals entering the Data Center to ensure these were authorized visitors.

Recommendation

We recommend GRU strengthen the visitor sign in sheet with a separate check off box indicating the visitor will be in the IT Data Center. This will allow management to determine when visitors have entered the data center and the purpose for that visit.

Management's Response

GRU IT has worked with the other GRU staff in charge of the visitor sign-in logs for the GRU Administration building and the GRU EOC System Control building to include the capturing of whether a visitor is going to be in a secure data center. GRU IT will also have a sign-in sheet located in each data center to be used if after hours escorted access is needed. We plan to have this fully implemented and communicated to staff by 4/30/2012.

ISSUE #3

Timely Completion of Incomplete Data Recovery Plan Elements

Discussion

During our review of GRU's DRP document, we noted that there were some broken or incomplete links within the document. GRU staff was aware of these deficiencies as broken links indicate "Fix Me" or question marks were noted within the document. These are noted by staff during maintenance routines or as updates are required. GRU attempts to make the noted corrections during the year as time becomes available.

NIST states a strong DRP should be complete, easy to follow and should allow for another IT trained employee unfamiliar with the specific disaster recovery plan to review it and execute the steps for recovery. Since a disaster or unexpected event can occur at any time, it is important that the DRP not have missing or incomplete information which may hinder the data recovery process.

Conclusion

The DRP has several incomplete links and contacts which make recovery of data more difficult if someone unfamiliar with the process has to step in to recover the data.

Recommendation

We recommend GRU correct the "Fix Me" and broken links within the DRP as soon as possible. As the DRP is a perpetual document, "Fix Me" links and contact lists will change during the life of the document. Management should allocate staff to correct and update corrections needed on a timely basis.

Management's Response

GRU IT remediated these documentation issues on 3/8/2012.