GALVESTON COUNTY

Office of County Auditor

Randall Rice CPA CISA CIO, County Auditor
Kristin Bulanek CIA, First Assistant County Auditor

P.O. Box 1418, Galveston, Texas 77553 **(409) 770-5304** **722 Moody Ave 4th Floor, Galveston, TX 77550**

July 13, 2020

Honorable Mark A. Henry, County Judge, and
Members of the Commissioners Court
722 Moody Avenue
Galveston, TX 77550

Honorable Mark A. Henry and Members of the Court:

Attached to be received and filed is the internal audit report of the Business Continuity and Disaster Recovery Plan Audit. The audit was performed from February 10, 2020 through June 15, 2020.

Sincerely,

Randall Rice CPA Digitally signed by Randall Rice CPA
Date: 2020.07.06 13:19:36 -05'00'

Randall Rice CPA
County Auditor

cc: Mr. Walter LaGrone

Attachment: Business Continuity and Disaster Recovery Plan Audit Report

June 15, 2020

To: Walter LaGrone
Chief Information Officer

From: Jordan Speer CIA CISA
IT Systems Auditor II

Re: Business Continuity and Disaster Recovery Plan Audit Report

The Internal Audit Division conducted an audit of the Information Technology Services (ITS) Department's Business Continuity and Disaster Recovery Plan as part of the current audit plan.

The objective of the audit was to evaluate the ITS Department's risk management and preparedness for recovery from significant business interruptions.

Background Information

According to the National Institute of Standards and Technology (NIST), business continuity is defined as an organization's ability to maintain essential functions during and after a disruption. A disaster recovery plan focuses on information systems and is designed to restore operability of systems, applications or computer infrastructure after an emergency.

The ITS Department drafted the Disaster Preparedness, Enterprise Continuity and Disaster Recovery Plan in 2017, and reviews the plan annually to ensure the plan is kept up to date. The auditor interviewed staff members, reviewed the 2019-2020 plan, revised in April 2019, the 2020-2021 plan, revised in April 2020, and researched best practices for business continuity and disaster recovery planning for this audit. The publications from NIST were the primary source used by the auditor in determining best practices. Publications from the Information Systems Audit and Control Association (ISACA) were also reviewed.

ITS Response: ITS drafted a DR Document in 2015. The document has undergone multiple revisions. At minimum, there is an annual revision. Each year there are lessons that are learned and the document accordingly is updated as required with those lessons learned. ITS agrees that NIST regulations and best practice is an excellent resource. ITS will consider your recommendations and will determine the right approach for Galveston County. ITS's complying with the FBI's Criminal Justice Information System (CJIS) policy and procedures. ITS subscribes to the Information Technology Information Library (ITIL) and will be reviewing and familiarizing the Health Insurance Portability and Accountability Act, HIPAA, policy and procedures.

Backup Procedures

According to NIST Publication 800-34-Contingency Planning, backup and recovery methods and strategies are a means to restore system operations quickly and effectively following a service disruption. Policies should specify the minimum frequency and scope of backups (daily or weekly, incremental or full) based on data criticality and the frequency that new information is introduced. Data backup policies should designate the location of stored data, file-naming conventions, media rotation frequency and method for transporting data offsite.

Finding: The auditor was unable to review the department's written backup and recovery procedures. A consulting firm, Berry Dunn McNeil & Parker, LLC, was hired during this review by the county to perform an audit of the ITS Department, which includes a scope to address disaster recovery. Due to this, ITS elected to not provide the policies and procedures to the auditor until after they are reviewed by the firm.

Recommendation BCDRP-20-01: The ITS Department should provide the existing written backup and recovery policies and procedures to Internal Audit for review for this audit report; once they have been reviewed by the consulting firm, a revised copy should be provided to Internal Audit.

ITS Response: It is unfortunate that your office did not receive any backup and recovery documentation. Attached are two of sixty ITS draft policies. Attached is the current backup retention procedures as well. ITS is looking to the consulting firm, BerryDunn, to review and if required, provide additional information to update the draft policies. ITS will submit the 60 draft policy for the Judge and Commissioners approval after BerryDunn recommendations.

Off-Site Storage Facilities

The security of the offsite storage facility should be evaluated to ensure it has the proper physical and environmental access controls. These controls include the following: the ability to limit access to only authorized users of the facility; the location of the offsite facility should be away from the primary data center, preferably in a facility that will not be subject to the same disaster event, to avoid the risk of a disaster affecting both facilities; and the facility should not be easily identified from the outside. This is to prevent intentional sabotage of the offsite facility should the destruction of the originating site be from a malicious attack. The facility should have adequate physical access controls, such as locked doors, no windows and active surveillance, among other controls.

There are several offsite storage facilities that house data centers at various locations around the county. The auditor visited each location to evaluate each site. All facilities appear to comply with industry best practices regarding offsite storage facilities.

ITS Response: ITS current backup strategy is disk to disk and replicate the backup file to another disk subsystem. The technology firm BerryDunn may recommend that ITS should re-invest in disk to disk to tape backup and restore infrastructure. ITS will consider your findings and recommendations and determine the right approach for Galveston County.

Disaster Recovery Plan

ISACA recommends the best practice for developing business continuity plans is to start by conducting a risk assessment. The risk is directly proportional to the impact on the organization and the probability of occurrence of the perceived threat. The result of the risk assessment should be the identification of the human resources, data, infrastructure elements and other resources (including those provided by third parties) that support the key processes, a list of potential vulnerabilities (the dangers or threats to the organization), the estimated probability of the occurrence of these threats and the efficiency and effectiveness of existing risk mitigation controls (risk countermeasures).

Finding: A documented risk assessment does not exist.

Recommendation BCDRP-20-02: The ITS Department should perform a documented risk assessment to ensure all potential risks and their likelihood and impact have been considered.

ITS Response: ITS will consider your findings and recommendation and will determine the right approach for Galveston County.

NIST Publication 800-34-Contingency Planning contains a seven step contingency planning process organizations can apply to develop and maintain a viable contingency planning program for their information systems. Step 2 is to conduct a business impact analysis (BIA). The BIA helps to identify and prioritize information systems and components critical to supporting the organization's mission/business processes.

The 2019-2020 ITS plan stated Business Impact Analysis (BIA) forms are used to identify critical systems and applications and establish recovery time objectives for restoring those systems and applications to operational status should a disruption occur. The forms state each department must perform a BIA on all critical functions. As BIA's are completed, their results should be incorporated into the plan. The updated 2020-2021 plan no longer contains the section regarding BIA’s.

Finding: While the updated plan no longer requires the BIA forms to be completed by each department, it is still best practice to conduct these analyses to identify and prioritize critical information systems and components. Without each department's cooperation, the ITS Department might not include a critical system in their disaster recovery efforts.

Recommendation BCDRP-20-03: The ITS Department should increase their efforts to encourage departments to submit information necessary for continuing business operations in the event of a disaster.

ITS Response: ITS will consider your findings and recommendations and determine the right approach for Galveston County.

NIST Publication 800-53, section CP-2 Contingency Plan, recommends the following as best practice: “Develop a contingency plan for the system that identifies essential missions and business functions and associated contingency requirements; provides recovery objectives, restoration priorities and metrics; addresses contingency roles, responsibilities, assigned individuals with contact information; addresses maintaining essential missions and business functions despite a system disruption, compromise or failure; addresses eventual, full system restoration without deterioration of the security and privacy controls originally planned and implemented; and is reviewed and approved by the appropriate personnel.”

Finding: The plan does not provide any metrics for recovery objectives and restoration priorities.

Recommendation BCDRP-20-04: The plan can be improved by identifying metrics to be used for measuring the success of the plan for future tests and actual disruptive events.

ITS Response: ITS will consider your findings and recommendations and determine the right approach for Galveston County.

In regards to training personnel, NIST Publication 800-34-Contingency Planning recommends the following: “Training for personnel with contingency plan responsibilities should focus on familiarizing them with their roles and teaching skills necessary to accomplish those roles. Training should be provided at least annually. Ultimately, personnel should be trained to the extent that they are able to execute their respective recovery roles and responsibilities without aid of the actual contingency plan document. This is an important goal in the event that paper or electronic versions of the plan are unavailable for the first few hours, as a result of the disruption.”

The 2019-2020 ITS plan stated a training program is to be developed by the Disaster Recovery (DR) Coordinator and ITS Management. The updated 2020-2021 plan expanded the training section to state there will be periodic training, at least twice annually, of ITS personnel regarding their roles in supporting this plan.

Finding: The training program and results of training are not documented, so the auditor was not able to perform a review of this area.

Recommendation BCDRP-20-05: The department should create a documented training program that will ensure ITS personnel are properly trained in disaster recovery activities. Support documentation for this training should be maintained as evidence the training occurred.

ITS Response: ITS does perform training. This year’s pre-hurricane season training was both interrupted and required ITS to limit the training due to the COVID response. A simulated storm exercise was conducted via email and a telephone conference bridge. All personnel, through the different escalation levels of their tier groups, and the associated responsibilities and provided a summary of how recovery would take place. We will document these activities better in the future. There is documentation associated with this training in the form of the emails. We also maintain a binder of after-action reports.

Per NIST Publication 800-34-Contingency Planning, testing is a critical element of a viable contingency capability. Testing enables plan deficiencies to be identified and addressed by validating one or more of the system components and the operability of the plan. A test plan should be developed and designed to examine the selected elements against explicit test objectives and success criteria. The use of test objectives and success criteria enable the effectiveness of each system and the overall plan to be assessed. Tests should mimic reality as closely as possible.

The 2019-2020 ITS plan stated, "Test all ITS Business Continuity Plans at least bi-annually to demonstrate the ability to achieve the BIA determined Recovery Time Objective”. The updated 2020-2021 plan no longer contains this statement.

Finding: The ITS Department is not performing tests of the plan.

Recommendation BCDRP-20-06: The ITS Department should conduct tests of the plan to ensure the plan is adequate in the event of an actual disruption.

ITS Response: ITS will consider your findings and recommendations and determine the right approach for Galveston County. ITS does perform situational testing if not twice a year, at least once a year. That situation will simulate a hurricane or a tropical storm and the technology team will talk about the required actions to take as the mock disaster moves forward. The team does not know what will transpire with the simulation so the team has to respond without prior knowledge of a condition, such as massive flooding or possible wind damage, or possible looting.

We wish to thank Mr. LaGrone and his staff for their cooperation and assistance.

cc: Randall Rice CPA, County Auditor
Kristin Bulanek CIA, First Assistant County Auditor