LEE COUNTY PORT AUTHORITY

Internal Audit Report

LCPA Information Technology – Service Recovery

Report Number: 2019.12
Date: July 11, 2019

LCPA Information Technology- Service Recovery

To: The Honorable Linda Doggett, Lee County Clerk of the Circuit Court & Comptroller
From: Tim Parks, Chief Internal Audit Officer/Inspector General
Date: July 11, 2019
Subject: LCPA Information Technology - Service Recovery Audit

Dear Ms. Doggett,

The Inspector General Department has completed an audit of LCPA Information Technology- Service Recovery. Bharat Vallarapu, CISA, CIA, CRISC, CRMA, Senior Internal Auditor conducted this review.

This audit activity conforms to the Institute of Internal Auditor's (IIA) *International Standards for the Professional Practice of Internal Auditing (Red Book)* and the Association of Inspectors General (AIG) *Principles and Standards for Offices of Inspector General (Green Book).*

The audit client's response is attached to this report. We wish to express our appreciation for the cooperation and assistance provided us by management and staff during this review.

This report will be posted to the Clerk of Courts website www.leeclerk.org under Inspector General Audit Reports. A link to this report has been sent to the Lee County Board of County Commissioners and appropriate parties.

Should you have any questions, please do not hesitate to contact me.

Sincerely,

Tim Parks

Tim Parks, CIA, CIG, CIGI,
Chief Internal Audit Officer/Inspector General
Inspector General Department

TJP/GK

LCPA Information Technology- Service Recovery

Table of Contents

Executive Summary 1
Background 1
Objective, Scope, and Methodology 2
Observations and Recommendations 2

LCPA Information Technology- Service Recovery

Executive Summary

The audit of the Lee County Port Authority (LCPA) Information Technology (IT) – Service Recovery function was included in the 2019 LCPA Annual Audit Plan as a carryover from 2018.

The IT risk factors were identified in a risk assessment questionnaire that was completed by department management. An entrance conference was held with management to discuss the results of the assessment, confirm the audit's objective and scope, and to solicit current information regarding risks.

The audit scope included review of LCPA IT policies and procedures related to Service Recovery (disaster recovery) - safeguarding of LCPA assets and LCPA data at the airport.

The LCPA IT Department has a critical service recovery management program with the objective of recovering infrastructure and data as a result of potential disasters and disruptive incidents.

Our conclusion is the LCPA IT Department's Disaster Recovery Plan (DRP) is satisfactory, and it mitigates risks associated with service recovery in the event of a disaster. The documentation of internal controls pertaining to overall IT policies, physical security, access management, and maintenance was satisfactory for service recovery by the Department.

We are confident that enhancing and formalizing specific DRP policies and procedures related to risk mitigation decisions, and clarifying the governance surrounding the decision making matrix would increase the probability of better outcomes in the recovery efforts of LCPA IT systems and its data in the event of a disaster.

Background

The LCPA IT Department provides Technology Lifecycle Management (TLM) for all technology infrastructures for Southwest Florida International Airport and Page Field General Aviation Airport. The TLM encompasses the planning, design, acquisition, implementation, and management of all the elements comprising the IT infrastructure.

The IT Department was comprised of two primary groups:

- Service Support - Manages and monitors IT processes necessary to ensure quality service to Service Desk and Airline Systems Support systems in common use, flight information, and parking.

- Service Design - Identifies service requirements and devises new service offerings as well as changes and improvements to existing ones in Systems Administration, Network Administration, and Desktop Design.

LCPA IT Department's Revenue for Fiscal Year 2018 (That run on IT Department Systems/IT infrastructure):

- Parking Lot - $17,379,428
- Common Use - $2,272,937
- Advertising - $664,103

Objective, Scope, and Methodology

The objective of the audit was to provide reasonable assurance of the effectiveness of program governance for the LCPA's Disaster Recovery Program.

The audit scope included review of LCPA IT policies and procedures related to Service Recovery (Disaster recovery) - safeguarding of LCPA assets and LCPA data at the airport.

The audit methodology was comprised of four steps:

- Preliminary Risk Assessment: Meeting was held with management to discuss the audit objective and scope.
- Planning: Audit procedures were developed based upon research, and audit objective, scope, and the preliminary meetings.
- Field Work – The Auditor
  - ✓ Reviewed the LCPA's DRP policies and procedures, interviewed LCPA IT management; and reviewed related documentation.
  - ✓ Evaluated and tested operations and procedures to address and complete the audit fieldwork.
  - ✓ Discussed and verified preliminary observations and findings with IT management.
- Wrap-up: An Exit Conference was held with management to discuss and obtain responses to the initial audit issues.

Observations and Recommendations

Disaster Recovery Plan

Disaster Recovery Plan (DRP) defines a disaster as an interruption or partial destruction of the computer, communication, and network environment within the primary data center that

will trigger the use of the secondary data center. Common risk factors leading to a disaster in a data center are hardware failure or fatigue, equipment damage by fire, flooding or mishandling, power brownouts or spikes, etc.

Based on the review:

- The DRP did not contain a policy denoting who in the LCPA had overall responsibility for the DRP. There was no chain of command stating who makes Disaster Recover (DR) decisions and coordinates in a disaster or emergency.
- There was no documentation of the steps for coordination, development, and maintenance of the DRP.
- There was no formal DRP committee or senior management approval for the DR status.
- There was not a documented process to evaluate whether new hardware of software should be included or removed from the DRP.

As a best practice:

- The DRP is created to provide governance of the DRP and testing procedures.
- The DRP states who is responsible for coordination, development, education, and maintenance.
- A DRP committee/board (Finance, Administration, Risk Management, etc.) is assembled for successful development and execution of the DRP.
- Policy steps require annual verification of the hardware and software requirements to be included or removed from the DRP.
- The policy details how the Department will manage and control any newly identified assets, risks in the DRP.

Without a fully developed DRP, the risk increases that management will be unable to provide a systematic approach for recovering the vital LCPA technology and data. The DRP provides a framework for the management, development, implementation, and maintenance of the LCPA assets. With a complete DRP, senior management can best ensure that sufficient financial, personnel and other resources will be available for the DRP.

Recommendation

We recommend that management create written DRP Policy and Procedures that outlines the DRP's governance, management, coordination, development, change management, and maintenance. We recommend that the DRP be approved by senior management.

DRP Maintenance

The DRP did not address a DRP Maintenance Strategy. We noted:

- There was no section to address the process to add or delete new applications or IT solutions in the DRP; and how to address the testing for those needs. There were no details in the plan on how often the DR procedures need to be reviewed or tested.
- The DRP steps and updates were not formally communicated to LCPA authorized staff. There was no documented evidence available to demonstrate compliance with the policy that the DRP were distributed to LCPA critical employees. The latest revisions in the DRP Plan that were updated in April 2019 were not distributed.
- There was no evidence of retention management. There were no instructions on how to discard old DRP plans upon creation of the new plans.
- Management did track the changes to the DRP plan but did not formally present and get them approved by the senior LCPA management team.

There was no evidence available to demonstrate compliance with the policy that the employees were trained and made aware of their roles in the DRP. Additionally, there were no details in the plan on how often the DRP testing needs to occur.

There was no evidence that the DRP plans or updates were communicated to LCPA employees.

Recommendation

We recommend that:

- The updates address if all the critical applications or IT solutions were included and tested in the DRP.
- The newly revised DRP plans are distributed or made available to all critical and authorized employees.
- Record management steps are referenced in the DRP, and only the current version of the DRP is retained.

DRP Lifecycle

There were no documentation details about the DRP's "focal point" with responsibility for overseeing DR activities in an event of an emergency.

The DRP did not identify at what point one DR phase of the DR incident would stop and when the next phase of the DR should start. Generally, the DR emergency management has continuous lifecycle. As a best practice, the DRP identifies who is responsible (focal point) to identify the transition between the DR phases of the DRP lifecycle.

Recommendation

We recommend that the DRP focal point be identified as responsible for declaring that normal operations may resume after an emergency. We recommend that the DRP be updated to identify the transitions between DR stages.

MEMO TO: Bharat Vallarapu
Senior Internal Auditor - IGD

FROM: Phillip Murray
Director, Information Technology Department

LEE COUNTY PORT AUTHORITY

DATE: July 3rd, 2019

SUBJECT: Audit Report Response

The following represents Lee County Port Authority staff comments and responses to the Internal Audit Report - Information Technology: Service Recovery.

Staff is pleased that the Senior Internal Auditor recognizes that the Disaster Recovery Plan (DRP) is solid and appreciates your comments to strengthen our Disaster Recovery program. The report was thorough and thoughtful and your recommendations will assist us in developing a sound Disaster Recovery Policy.

We have the following comments

"There was no chain of command stating who makes Disaster Recover (DR) decisions and coordinates in a disaster or emergency"

Section 8, page 9, first paragraph of the DRP describes the Disaster Recovery Call Tree and states DR Team Leader invokes plan and ensures alternate site working. It is important to understand that the LCPA DR system takes approximately 5 minutes to move all critical systems from the primary data center to the secondary data center (alternate site). Once the plan is invoked by the DR Team Leader, there are no further deliberations required or possible.

"There was no documentation of the steps for coordination, development, and maintenance of the DRP"

Section 10 titled Plan Maintenance describes suggested steps to maintain the plan.

"There was not a documented process available to demonstrate compliance with the policy to annually verify the hardware and software requirements"

This statement is not clear. It does not identify which system staff should verify requirements for; the DR system itself, or the systems protected by the DR system. If the Auditor is referring to the DR system itself, then staff feels the process of the annual testing detailed in section 9, Plan Testing, meets this requirement. If the Auditor is referring to the systems projected by the DR system, then addressing the following finding should suffice.

"There was no section to address the process to add or delete new applications or IT solutions in the DRP; and how to address the testing for those needs. There were no details in the plan on how often the DR procedures need to be reviewed or tested"

Section 10 Plan Maintenance states "The IT DRP is reviewed at least once a year or any time a major system update or upgrade is performed, whichever is more often."

There is no mention in the Auditor's report of the document titled "LCPA - IT Disaster Recovery Plan - Annual Test Procedures" which addresses how the DRP test should be conducted. The takeaway by staff is that the policy document should clearly describe a process for reviewing if new systems acquired by the Port Authority need to included in the DRP and if existing systems should be removed.

"The latest revisions in the DRP Plan that were updated in April 2019 were not distributed"

The DRP is in a shared folder that all involved IT staff have read access to. Staff does not wish to distribute copies which consume storage space and create confusion as to which copy of the DRP is current. However, the Auditor is correct that some staff may not have been alerted that the plan had been updated. Staff will incorporate language into the policy document that requires a notification process when the DRP is updated.

"There were no documentation details about the DRP's "focal point" with responsibility for overseeing DR activities in an event of an emergency"

Plan states DR Team Leader is responsible to invoke the plan. Staff will add the description "focal point" to the policy document and language to more fully clarify the DR Team Leader's role.

"There was no evidence available to demonstrate compliance with the policy that the employees were trained and made aware of their roles in the DRP"

Staff will add language to the policy document that addresses this finding.

"Additionally, there were no details in the plan on how often the DRP testing needs to occur"

Section 9 Plan Testing states testing should occur once a year. Language will be added to the policy document that adds that testing should also occur when new systems are added to the DR system.

"The DRP did not identify at what point one DR phase of the DR incident would stop and when the next phase of the DR should start"

Port Authority DR system is highly automated. Once failover is invoked, no staff intervention is required. This finding does highlight that there is not a policy statement to address when and under what circumstances staff should fail back to the primary data center. Staff will develop language to address this finding.

"As a best practice, the DRP identifies who is responsible (focal point) to identify the transition between the DR phases of the DRP lifecycle"

DRP states DR team leader is responsible for invoking the plan.

Recommendation

"We recommend that management create written DRP Policy and Procedures that outlines the DRP's governance, management, coordination, development, change management, and maintenance. We recommend that the DRP be approved by senior management."

Port Authority staff will develop a DRP Policy document that clearly outlines policy and procedure to govern and maintain the Disaster Recovery Plan as suggested.

We recommend that:

- *The updates address if all the critical applications or IT solutions were included and tested in the DRP.*
- *The newly revised DRP plans are distributed or made available to all critical and authorized employees.*
- *Record management steps are referenced in the DRP, and only the current version of*

the DRP is retained.

Port Authority will include these recommendations in the DRP Policy guide.

Recommendation

"We recommend that the DRP focal point be identified as responsible for declaring that normal operations may resume after an emergency. We recommend that the DRP be updated to identify the transitions between DR stages"

DR team leader is identified. Port Authority will add language requiring DR team leader to inform leadership and customers that normal business may proceed.

Thank you again for the opportunity to furnish comments on the Internal Audit Report for Information Technology Service Recovery for the Lee County Port Authority.

IT estimates it will take 9 months to create a Disaster Recovery Plan Policy document and procedures to address the findings of this report.

CC: Jeff Mulder
Benjamin Siegel
Brian McGonagle