

ITS Continuity and Disaster Recovery Planning

Internal Audit Report
November 1, 2019



Linda J. Lindsey, CPA, CGAP, Senior Director
Jan N. Skjersaa, CPA, Internal Auditor
Luis E. Aponte Santiago, CISA, IT Internal Auditor

Table of Contents

	Page Number
EXECUTIVE SUMMARY	1
BACKGROUND	2
OBJECTIVE, SCOPE, AND METHODOLOGY	3
BEST PRACTICES	4
RESULTS AND RECOMMENDATIONS	5
APPENDIX A	7

EXECUTIVE SUMMARY

Why We Did This Audit

The objective of this audit was to determine the degree of ITS preparedness in the event of operational disruptions, staff absences, turnover, and other unforeseen / emergency conditions.

This is a planned engagement derived from the annual audit risk assessment process. This audit was included in the 2017-2018 Annual Audit Plan.

- The department has made a start on an ITS Disaster Recovery plan
- No ITS Continuity of Operations Plan has been prepared

Our overall conclusion is that ITS:

- has the beginning of a IT Disaster Recovery plan but needs to continue to develop and maintain it
- needs to prepare and maintain a Continuity of Operations Plan

Observations and Conclusions

Audit Results at a Glance			
Results and Observations	Risk / Impact Rating		
	Significant	Moderate	Minor
IA - Internal Audit or M - Management	M - 3	IA - 1	--
D - Deficiency or O - Opportunity	D - 3	D - 1	--

We noted that:

- There is no written policy to guide the Information Technology Services (ITS) Department Continuity of Operations and Disaster Recovery activities
- The department has not performed a Business Impact Analysis

Results and Recommendations

As a result of our audit, we recommend that the following be prepared:

- An IT Continuity of Operations and Disaster Recovery policy
- A Business Impact Analysis (BIA)
- A complete and current ITS Continuity of Operations Plan (COOP)
- A complete and current ITS Disaster Recovery plan

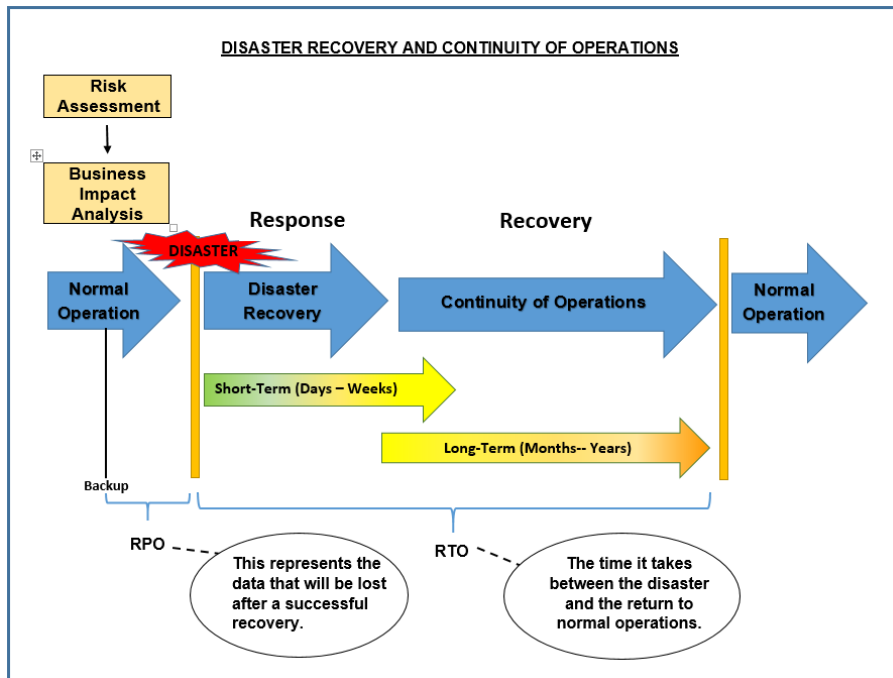
This report has been discussed with management and they have prepared their response, which follows.

BACKGROUND:

In these days of increasing natural disasters (i.e. hurricanes), hackers, malware, ransomware and other threats, it is important that the district's IT function have an effective and implementable plan to recover and continue operations during and after these types of events. The subject of this audit was identified as a high priority in the audit risk assessment and is a focus area of the Audit Advisory Committee. As noted in our audit of Emergency Management and Business Continuity, the district as a whole has performed a certain amount of business continuity and disaster recovery planning but, since technology pervades our operations, much of its success is dependent on an effective IT plan. This engagement focused on the Information Technology Services (ITS) Department's part of the plan.

Planning for recovery from disasters and achieving continuity of operations should be an integral part of the strategic objectives of an organization. The chart below shows the various processes, and their sequence, needed to prepare and recover from an adverse event.

Diagram 1 –Disaster Recovery and Continuity of Operations



Source: GTAG – Business Continuity Management

An effective and implementable IT plan to recover and continue operations is essential.

Disaster Recovery and Continuity of Operations diagram

ITS Continuity and Disaster Recovery Planning Internal Audit Report

OBJECTIVE, SCOPE AND METHODOLOGY:

Objective

The objective of this audit was to determine the degree of ITS preparedness in the event of operational disruptions, staff absences, turnover, and other unforeseen / emergency conditions.

Scope

The scope of the audit addressed the ITS plans as they existed at the time of our audit (the 2018-2019 fiscal year).

Methodology

This audit looked at the Disaster Recovery and Continuity of Operations plans. We assessed whether departmental management has set a guiding policy, the methodology used for implementation, how extensive or detailed the plans are, how current the plans are, and whether the plans are tested. Our audit methodology included:

- interviewing personnel of the ITS Department;
- reviewing School Board Policies and departmental procedures;
- reviewing the Disaster Recovery documents; and,
- researching best practices: *Business Continuity Management: GTAG – Global Technology Audit guide – IPPF-Practice Guide* by David Everest, Roy E. Garber, Michael Keating, Brian Peterson (July 2008) and *NIST Special Publication 800-34 Rev. 1 – Contingency Planning guide for Federal Information Systems* by Marianne Swanson, Pauline Bowen, Amy Wohl Phillips, Dean Gallup, David Lynes (May 2010))

Our audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* of the Institute of Internal Auditors and included such procedures as deemed necessary to provide reasonable assurance regarding the objective. Internal Auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes. We are required to note any material deficiencies in accordance with Florida Statutes, School Board Policy and sound business practices. We also offer

We determined the degree of ITS preparedness for operational disruptions

Types of planning assessed in this audit:

- *Disaster Recovery*
- *Continuity of Operations*

This audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

suggestions to improve controls or operational efficiency and effectiveness.

BEST PRACTICES – IT CONTINUITY & DISASTER RECOVERY PLANS

The purpose of preparing for an adverse event is to reduce the adverse impact upon the organization and shorten the amount of time it would take to resume normal operations. It is as important to prepare at a departmental level as it is at the District level. The following sequential activities¹ are commonly recommended practices needed to prepare an organization for an adverse event:

- Developing a Guiding Departmental Policy – this guides the subsequent departmental planning for an adverse event
- Performing a Risk Assessment – an assessment of potential disruptive events ranging from natural disasters (e.g. hurricanes, flooding) to industrial accidents (e.g. fires, explosions) to supplier failures (e.g. electricity loss, loss of access to cloud data) to labor disruption (e.g. strikes, transportation)
- Performing a Business Impact Analysis (BIA) – an analysis of the impact to the organization of each likely disruptive event as determined by the Risk Assessment
- Plan development and strategy implementation based upon the BIA
 - Develop the Disaster Recovery plan – the actions to perform to restore IT systems, and other related systems, to the most recently backup-up state
 - Develop the Continuity of Operations plan – a longer-term plan, which addresses issues such as the priority of critical business processes to be recovered, critical vendor contact information, dependent departments, moving to an alternate location, list of key personnel and their backups if needed, and other issues
- Communication and Training of the plans – Communicate the plans so all are informed and trained to perform their functions when plans are implemented

Activities recommended in establishing an IT Disaster Recovery and Continuity of Operations Plan

Disaster Recovery plan – the actions to perform to restore IT systems to the most recently backed-up state

Continuity of Operations plan – steps to restore a previously determined level of operations during the emergency

¹ NIST Special Publication 800-34 Rev. 1, p. ES-1

- Testing of the plans – Testing validates that the plans will work when they are needed
- Maintenance of the plans – Periodic maintenance will ensure they will be current when needed

Maturity models are frequently used to evaluate capability and discover gaps between current and desired states. We adapted the Business Continuity Maturity Model in the GTAG mentioned previously for an assessment of ITS' current state as compared to characteristics of capability in several key aspects of the business continuity and disaster recovery planning processes. (See Appendix A for the "Process Maturity" model.)

RESULTS & RECOMMENDATIONS:

1) There is no written policy to guide Information Technology Services (ITS) Disaster Recovery Policy and Continuity of Operations activities. *Moderate Risk / Internal Audit*

Audit Results:

There is no department-approved policy to guide the ITS Continuity of Operations and Disaster Recovery activities. Such a policy will provide the framework upon which detailed procedures will be developed.

Recommendation:

Prepare a written and approved ITS Continuity and Disaster Recovery policy.

2) No Business Impact Analysis has been performed. *Significant Risk / Management*

Audit Results:

The ITS department has not performed a Business Impact Analysis; however, we were informed that a worksheet is being developed for that purpose. The intent is to distribute the worksheet to the various district departments supported by ITS to ascertain each department's mission critical processes and prioritize them. After this worksheet is completed by each of the other departments and returned to ITS, the department will better know the full extent they are relied upon to

A departmental-approved ITS Disaster Recovery and Continuity of Operations policy has not been prepared.

No Business Impact Analysis has been performed.

provide services. The ITS department's BIA can then identify the type of business impact that will occur if one or more of their processes cannot be performed.

Recommendation:

Perform a Business Impact Analysis for ITS and update it periodically.

3) The Disaster Recovery Plan is incomplete. *Significant Risk / Management*

Audit Results:

ITS does not have a written Disaster Recovery Plan (DRP). They have some procedures but not a complete plan. They have procedures:

- for the first steps in a planned disaster (an example is a hurricane where you have several days to prepare), and
- to take for an unplanned disaster.

These procedures should be included in a comprehensive, well-documented and well-tested DRP for ITS.

Recommendation:

Prepare and maintain a well-documented and well-tested Disaster Recovery Plan.

4) A Continuity of Operations Plan is needed. *Significant Risk / Management*

Audit Results:

There is no Continuity of Operations Plan (COOP) in place in case of an adverse event.

Recommendation:


A well-documented and well-tested COOP should be developed and maintained.

We wish to thank the staff of the Information Technology Services and Risk Management Departments for their cooperation and assistance with this audit.

A well-documented and well-tested Disaster Recovery Plan is critical ITS has some disaster recovery procedures but not a complete DRP

ITS Continuity and Disaster Recovery Planning Internal Audit Report

Appendix A – Process Maturity Model

						
Objective	Level 1 Initial	Level 2 Repeatable	Level 3 Defined	Level 4 Managed	Level 5 Optimizing	ITS Current Status and Assessed Level of Maturity
Guiding Departmental Policy	Management has not developed a policy.	Management has informally developed policy.	There is a formal policy, but it is not up-to-date.	Formal policy is maintained on an as-needed basis.	Policy is up-to-date and regularly maintained.	No department policy has been prepared.
Risk Assessment	Neither a formal nor informal risk assessment has been performed.	Management has informally developed risk assessment conclusions.	A more informal approach has been implemented regarding assessing risk.	The risk assessment process takes into account controls assessment. This process is repeatable and is executed on a regularly scheduled basis.	The results of periodic risk assessment drive continued enhancement to recovery strategies.	Started, but not complete 1
Business Impact Analysis (BIA)	Neither a formal nor informal Business Impact Analysis has been performed.	Management has informally developed recovery priorities.	Management has identified an approach to define levels of criticality, supporting a methodology to collect/estimate business impact data.	The establishment of objectives and effectiveness are measurable. Both recovery time objectives (RTO) and recovery point (data loss tolerance) objectives (RPO) are established.	The execution and review of BIA's are coordinated with organizational and technology change management/due diligence processes.	Started, but not complete 1
Plan Development and Strategy Implementation	Plans are often out of date, if available.	Plans are often updated in an ad hoc manner.	Continuity of operations plans and IT disaster recovery plans are documented and include organizational detail.	Plans are maintained on an as-needed basis, as opposed to a minimal standard (e.g. annually).	Crisis, disaster recovery, and business resumption plans are integrated in planning and execution.	Started, but not complete 1
Communication and Training	No formal communication or training program exists. Only those with immediate responsibility know program goals and objectives.	Specific program components may have designated backups, and team members are included in casual communication regarding the program.	Employees beyond the planning and execution teams understand the program goals and objectives.	Employees know their immediate responsibilities in an actual event, and many know their long-term activities.	A deep understanding of the BC program and its impact on daily operations is understood by all layers of the organization.	Daily, weekly, and other periodic backups are performed. 2
Testing and Plan Maintenance	IT component testing takes place internally within the IT department. Plans may not be well maintained or up-to-date because the BC process is new.	In some organizations, management engages in scenario-driven, tabletop exercises of its CM capabilities. IT disaster recovery tests are focused on component recovery.	BC and IT disaster recovery tests are sometimes performed together, but the focus is typically on component recovery.	Full BC testing, for business and IT, are regularly performed.	BC testing is unannounced. Entire department works at an alternate site for a defined period of time using backup systems and resources.	There is testing at an alternate location annually. 2
Adapted from: Business Continuity Management – GTAG – Global Technology Audit Guide, IPPF – Practice Guide, Appendix						



Department / School Name	ITS
Administrator / Department Head	Russell Holmes
Cabinet Official / Area Superintendent	Robert Curran

Exception Noted (Finding / recommendation) What is? What should be?	Management Response (Corrective Action) What needs to be done?	Responsible Person (Name & Title) Who needs to do it?	Expected Outcome & Completion Date What is the evidence of the corrective action? When will the action be completed? (MM/YYYY)
An IT Continuity of Operations and Disaster Recovery policy	We agree that planning for unforeseen events is an important part of ITS Operations. Documentation from previous ITS leadership cannot be located.	Russell Holmes, Sr. Director of Information Security	Completion of a Disaster Recovery and Continuity of Operations Plan. 06/2020 (goal, have completed by the beginning of next hurricane season)
A Business Impact Analysis (BIA)	We agree that planning for unforeseen events is an important part of ITS Operations. Documentation from previous ITS leadership cannot be located.	Russell Holmes, Sr. Director of Information Security	A Business Impact Analysis is currently underway. 05/2020
A complete and current ITS Continuity of Operations Plan (COOP)	We agree that planning for unforeseen events is an important part of ITS Operations. Documentation from previous ITS leadership cannot be located.	Russell Holmes, Sr. Director of Information Security	Completion of a Disaster Recovery and Continuity of Operations Plan. 06/2020 (goal, have completed by the beginning of next hurricane season)



A complete and current ITS Disaster Recovery plan	We agree that planning for unforeseen events is an important part of ITS Operations. Documentation from previous ITS leadership cannot be located.	Russell Holmes, Sr. Director of Information Security	Completion of a Disaster Recovery and Continuity of Operations Plan. 06/2020 (goal, have completed by the beginning of next hurricane season)
---	--	--	---