

**OFFICE OF THE AUDITOR GENERAL**

**The Navajo Nation**

**A Follow-up Review  
of the  
Office of the Controller  
Disaster Recovery Plan  
Corrective Action Plan Implementation**


**Report No. 17-13  
January 2017**

Performed by:  
Jeanine Jones, Senior Auditor  
Alfreda Lee, Senior Auditor



**M-E-M-O-R-A-N-D-U-M**

**TO** : Bobby White, Acting Controller  
**OFFICE OF THE CONTROLLER**

**FROM** :   
Elizabeth Begay, CIA, CFE  
Auditor General  
**OFFICE OF THE AUDITOR GENERAL**

**DATE** : January 11, 2017

**SUBJECT** : A Follow-up Review of the Office of the Controller Disaster Recovery Plan Corrective Action Implementation

The Office of the Auditor General herewith transmits Audit Report no. 17-13, A Follow-up Review of the Office of the Controller Disaster Recovery Plan Corrective Action Implementation. The follow-up was conducted to determine the status of the corrective action plan, which was developed by the Office of the Controller in response to the 2010 audit of the Financial Management Information System (FMIS) Disaster Recovery Plan. The FMIS Project Manager within the Office of the Controller is the administrator of the Disaster Recovery Plan. The 2010 audit report and the corrective action plan were approved by the Budget and Finance Committee on July 6, 2011 per resolution BFJY-16-11.

**FOLLOW-UP RESULTS**

Prior Findings	Number of CAP Components <u>IMPLEMENTED</u>	Number of CAP Components <u>NOT IMPLEMENTED</u>	Audit Issue Adequately Resolved?
Lack of a comprehensive FMIS disaster recovery plan.	2	2	Yes
A comprehensive inventory list of FMIS information technology software for disaster recovery is not maintained.	4	0	Yes
Lack of a certified FMIS computer hardware for disaster recovery.	3	0	Yes
Funding of a disaster recovery program is not adequate.	5	0	Yes
Lack of service level agreements with major FMIS users.	0	3	No
The FMIS data center is not adequately protected.	2	0	Yes
There is no assurance that the FMIS information technology equipment is properly insured.	3	0	Yes
<b>Total</b>	<b>19 Implemented</b>	<b>5 Not Implemented</b>	

Memo to Bobby White

Page 2

**CONCLUSION**

The Office of the Controller has implemented 19 out of 24 corrective measures from the corrective action plan approved by the Budget and Finance Committee on July 6, 2011 per resolution BFJY-16-11. In doing so, the Office of the Controller's FMIS Information Technology Section has reasonably addressed the audit findings from the 2010 audit of the Financial Management Information System Disaster Recovery Plan. Therefore, the Office of the Auditor General does not recommend sanctions on the Office of the Controller in accordance with 12 N.N.C. Section 9.

xc: Laura Johnson, FMIS Project Manager  
Lorena Eldridge, Accounting Manager  
**OFFICE OF THE CONTROLLER**  
Chrono

## Table of Contents

	<u>Page</u>
INTRODUCTION AND BACKGROUND	1
PROGRAM PURPOSE AND ORGANIZATION	1
OBJECTIVE, SCOPE, AND METHODOLOGY	2
PRIOR FINDINGS, PRIOR RECOMMENDATIONS AND CURRENT STATUS	3

## **INTRODUCTION AND BACKGROUND**

The Office of the Auditor General conducted a special review of the Office of the Controller in 2010 and issued audit report no. 10-11. The objective of the review was to determine if a comprehensive disaster recovery plan has been developed by the Office of the Controller and whether business continuity risks are mitigated in the event of catastrophic events such as fire, in-house flooding, sabotage, physical theft, technology and security intrusions, and hardware failures.

The 2010 special review resulted in seven significant findings with related recommendations. The review found the Office of the Controller's:

- 1) comprehensive Financial Management Information System disaster recovery plan was lacking,
- 2) comprehensive inventory list of Financial Management Information System information technology software for disaster recovery was not maintained,
- 3) certified Financial Management Information System computer hardware for disaster recovery was lacking,
- 4) disaster recovery program funding was not adequate,
- 5) service level agreements with major Financial Management Information System users were lacking,
- 6) Financial Management Information System data center was not adequately protected, and
- 7) Financial Management Information System information technology equipment was not properly insured.

The audit report and corrective action plan developed by the Office of the Controller were approved by the Budget and Finance Committee on July 6, 2011 per resolution no. BFFY-16-11.

## **PROGRAM PURPOSE AND ORGANIZATION**

The Office of the Controller currently manages the Financial Management Information System which is the Navajo Nation's core operation for automated financial information processing. The Financial Management Information System Project Manager and technical support staff are responsible for the day-to-day operations and provide support activities for the Financial Management Information System.

The Financial Management Information System was implemented in fiscal year 2003 and is an integrated suite of software applications which includes account receivable, procurement, property and general ledger modules providing functionality to interact and provide real-time financial information of the Navajo Nation.

## OBJECTIVE, SCOPE, AND METHODOLOGY

In accordance with 12 N.N.C., Section 7, the following objective was established for the follow-up review:

- Determine whether the Office of the Controller implemented its approved corrective action plan.

The follow-up primarily focused on the approved corrective action plan. However, if other significant issues were noted during the review, such issues were further evaluated for materiality and risk to determine whether the issues warranted presentation in this report. Any issues of materiality and risk could have an adverse effect on the program operations and hinder the achievement of program goals and objectives.

To meet the objective, we performed the following procedures:

- Reviewed the Disaster Recovery Plan for completeness.
- Interviewed Office of the Controller staff including the System Project Manager, Application Specialist, and Accounting Managers.
- Reviewed consultant contract for the type of assistance provided to the Office of the Controller with the implementation of disaster recovery.
- Reviewed vendor contract for the designated hot site in Albuquerque, New Mexico.
- Selected a sample of 64 software and hardware assets from a total population of 638 to verify the software/hardware information and location corresponded to the inventory listing maintained by the Office of the Controller.
- Evaluated budgets and loan agreement for funding of disaster recovery from fiscal year 2014 to fiscal year 2016.
- Verified service level agreements with major Financial Management Information System users are in place.
- Verified with Navajo Nation Department of Information Technology that the server located in Window Rock, Arizona is adequately protected.
- Verified the equipment for the designated hot site located in Albuquerque, New Mexico is adequately protected.
- Verified through Navajo Nation Risk Management Department that the Financial Management Information System software and hardware are insured.

The scope for this follow-up review was for the period beginning January 1, 2016 through November 1, 2016. The audit sampling was done using judgmental sampling methods.

The Office of the Auditor General expresses their appreciation to the Office of the Controller staff and all other entities who contributed to this audit for their cooperation and assistance through the audit.

**REVIEW RESULTS**  
**PRIOR FINDINGS, RECOMMENDATIONS AND CURRENT STATUS**

**Prior Finding I: Lack of a comprehensive Financial Management Information System Disaster Recovery Plan.**

The prior finding stated the Office of the Controller did not develop a comprehensive Disaster Recovery Plan that will meet the general requirements of continuing business if disaster occurs, for instance, fire, in-house flooding, sabotage, physical theft, technology and security intrusions and hardware failures.

<b>Corrective Actions</b>	<b>Current Status of Corrective Actions</b>
<p>1.1. The Office of the Controller will develop a comprehensive Disaster Recovery Plan and a comprehensive business continuity framework. The plan will include but not limited to the following components:</p> <ol style="list-style-type: none"> <li>1) Information Technology Statement of Intent - This sets the stage and direction for the plan.</li> <li>2) Policy Statement - An approved statement of policy regarding the provision of disaster recovery services.</li> <li>3) Objectives - Main goals of the plan.</li> <li>4) Key Personnel Contact Information - Key information most likely to be used right away, and should be easy to locate.</li> <li>5) Plan Overview - Describes basic aspects of the plan, such as updating.</li> <li>6) Emergency Response - Describes what needs to be done immediately following the onset of an incident.</li> <li>7) Disaster recovery team - Members and contact information of the disaster recovery team.</li> <li>8) Emergency Alert, Escalation and Disaster Recovery Plan Activation - Steps to take through the early phase of the incident, leading to activation of the Disaster Recovery Plan.</li> <li>9) Media - Tips for dealing with the media.</li> <li>10) Insurance - Summarizes the insurance coverage associated with the Information Technology environment and any other relevant policies.</li> <li>11) Financial and Legal Issues - Actions to</li> </ol>	<p><b>Implemented</b></p>

<p>take for dealing with financial and legal issues.</p> <p>12) Disaster Recovery Plan Exercising - Underscores the importance of the disaster recovery plan exercising.</p>	
<p>1.2. The Office of the Controller will cooperate with major Financial Management Information System users in plan development by communicating thru meetings and discussions.</p>	<p><b><u>Not Implemented.</u></b> There were no records of meetings or discussions to show the Office of the Controller cooperated with major Financial Management Information System users in the Disaster Recovery Plan development. Rather, the Office of the Controller used a disaster recovery template obtained from the Internet to develop the Disaster Recovery Plan. In the absence of clear communication in the development of the Disaster Recovery Plan, the Office of the Controller cannot provide assurance users had input developing the plan and they fully understand their duties in implementing the Disaster Recovery Plan.</p>
<p>1.3. The Office of the Controller will conduct a cost/benefit analysis to meet an efficient and effective Disaster Recovery Plan establishing a cold, warm or hot site.</p>	<p><b>Implemented</b></p>
<p>1.4. The Office of the Controller will begin to develop an overall Information Technology Governance Plan for the Office of the Controller.</p>	<p><b><u>Not Implemented.</u></b> The Office of the Controller provided an Information Technology Governance Plan. However the plan is incomplete and needs more development. Consequently, the Office of the Controller cannot provide assurance its information technology strategy aligns with its business strategy to ensure the Office of the Controller stays on track to achieve its overall goals and objectives, and provides a way for the Office of the Controller to measure its information technology performance.</p>
<p><b>Audit Finding Resolved? Yes</b></p>	



**Prior Finding II: A comprehensive inventory list of software for disaster recovery for the Financial Management Information System Information is not maintained.**

The prior finding stated the Office of the Controller does not maintain a complete and accurate software inventory of the Financial Management Information System software assets for disaster recovery. The Financial Management Information System computer software, which is the JD Edward Enterprise One, is not identified in the inventory listing by the Office of the Controller. There is no classification of essential software nor an indication of their status as licensed products. Lastly, the software inventory does not include a comprehensive list of software license agreements, terms and conditions, validations, certifications and signatures attesting to their content and completeness that would be used for disaster recovery.

<b>Corrective Actions</b>	<b>Current Status of Corrective Actions</b>
2.1. A disaster recovery software inventory listing will be prepared and updated annually for all software that is needed to restart services. The list will be certified, signed, and dated by Financial Management Information System Project Manager and Controller.	<b>Implemented</b>
2.2. The listing will be a detailed listing with the following information: 1) Description 2) Version 3) License date 4) Support warranty 5) Expiration date 6) Original cost 7) Disaster recovery cost 8) Serial number or reference number 9) Additional identifying number	<b>Implemented</b>
2.3. The Office of the Controller will develop an assurance process for compliance with software licensing agreements and standards.	<b>Implemented</b>
2.4. The Office of the Controller will assign Financial Management Information System technical support staff to software maintenance and responsibilities for disaster recovery activities.	<b>Implemented</b>
<b>Audit Finding Resolved? Yes</b>	

**Prior Finding III: Lack of certified Financial Management Information System computer hardware for disaster recovery.**

The prior finding stated the Office of the Controller does not maintain a listing of critical Financial Management Information System computer and network infrastructure equipment for disaster recovery. The inventory list is necessary to rebuild the Financial Management Information System computer operations if a disaster occurs.

<b>Corrective Actions</b>	<b>Current Status of Corrective Actions</b>
3.1. The Financial Management Information System disaster recovery equipment inventory will be prepared and updated annually. This inventory will be certified and signed by the Financial Management Information System Project Manager and the Controller.	<b>Implemented</b>
3.2. The listing will contain the following components: 1) Hardware Description 2) Property/Serial No. 3) Equipment Type 4) Cost 5) Verification Date and Signature	<b>Implemented</b>
3.3. The Office of the Controller Property Management department will conduct a perpetual inventory and maintain a comprehensive list.	<b>Implemented</b>
<b>Audit Finding Resolved? Yes</b>	

**Prior Finding IV: Funding of a disaster recovery program is not adequate.**

The prior finding stated the Office of the Controller’s operating and fixed cost budgets for fiscal year 2008 and 2009 do not include costs or contingency plans for disaster recovery activities other than computer system backups. There are no budget policies in place to assure major Financial Management Information System users that their operations are not jeopardized and placed at risk after a disaster occurrence.

<b>Corrective Actions</b>	<b>Current Status of Corrective Actions</b>
4.1. The Navajo Nation shall provide funding for an appropriate Disaster Recovery Plan.	<b>Implemented</b>
4.2. The Office of the Controller will attempt to obtain funding for budgeting purposes. Funding requests via memorandums and disaster recovery budget will be sent to the Office of Management and Budget and Office of the President/Vice-President.	<b>Implemented</b>
4.3. A budget presentation will be provided to the Executive Branch Budget Team.	<b>Implemented</b>
4.4. The Office of the Controller will establish a disaster recovery budget for the Financial Management Information System.	<b>Implemented</b>
4.5. The Office of the Controller will establish the disaster recovery project and develop performance measures and timelines.	<b>Implemented</b>
<b>Audit Finding Resolved? Yes</b>	

**Prior Finding V: Lack of service level agreements with major Financial Management Information System users.**

The prior finding stated the Office of the Controller did not provide service level agreements with major Financial Management Information System users that define customer requirements and information technology capabilities. The major Financial Management Information System users consists of tribal programs and departments with critical health, social, emergency type operations such as Office of Navajo Scholarship and Financial Assistance, Division of Social Services, Program for Self-Reliance, and Public Safety. Disaster recovery activities such as planning, consultation, assurances and/or coordination efforts are lacking or non-existent with major Financial Management Information System users.

Corrective Actions	Current Status of Corrective Actions
<p>5.1. The Office of the Controller will implement disaster recovery service level agreements with major Financial Management Information System users such as Scholarship Office, General Assistance, and Temporary Assistance for Needy Families.</p>	<p><b>Not Implemented.</b> Major users are tribal programs and departments that provide critical health, safety and emergency services for the Navajo Nation. Service level agreements for the Division of Social Services and the Scholarship Office were provided but since the Office of the Controller did not provide a list of all major users of the Financial Management Information System, there is no assurance that service level agreements have been implemented for all major users.</p>
<p>5.2. The service level agreements will contain the following:            1) Services            2) Priorities            3) Responsibilities</p>	<p><b>Not Implemented.</b> The service level agreements for the Division of Social Services and the Scholarship Office contain general terms and did not specifically address the three areas noted in the corrective action plan: services, priorities and responsibilities. Rather, the agreements addressed performance, communication, and uninterrupted services without specific details. The agreements do not clearly explain how the Office of the Controller and each major user will respond to a disaster and how they will plan, coordinate and recover from such a disaster. There is a risk that, in the absence of specific details, there will be confusion, misunderstandings and delays with the disaster recovery efforts.</p>
<p>5.3. The service level agreements will include an agreement for disaster recovery.</p>	<p><b>Not Implemented.</b> The service level agreements that were provided by the Office of the Controller did not include specific provisions to address disaster recovery. There was no information for the major users to use in case of a disaster and agreed-upon procedures between the major users and the Office of the Controller in responding to the disaster.</p>
<p><b>Audit Finding Resolved? No</b></p>	

**Prior Finding VI: The Financial Management Information System data center is not adequately protected.**

The prior finding stated the Financial Management Information System data center is not adequately safeguarded in the event of a fire and the Financial Management Information System data center is being used to store other goods and equipment not pertinent to the Financial Management Information System that are fire hazards. The equipment is not protected from fire in accordance with information technology standards cited from the National Fire Protection Association standard 75. The Financial Management Information System data center does not have an operable fire suppression system. Furthermore, a water based fire suppression system does not meet the standards for information technology equipment. Although, a portable gaseous suppression unit was acquired by Office of the Controller, such system may only perform momentarily while a fire erupts in the surrounding areas.

<b>Corrective Actions</b>	<b>Current Status of Corrective Actions</b>
6.1. The Office of the Controller will install an operable fire suppression system.	<b>Implemented</b>
6.2. The Office of the Controller will remove goods and equipment not related to Financial Management Information System.	<b>Implemented</b>
<b>Audit Finding Resolved? Yes</b>	

**Prior Finding VII: There is no assurance that the Financial Management Information System Information Technology equipment is properly insured.**

The prior finding stated the Office of the Controller did not submit the 2010 Risk Management Property Schedule listing, in detail, the Financial Management Information System computer equipment and the purchase costs, fair market value or replacement costs. Consequently, there is no verifiable computer listing to be used for insurance claims and recovery in the event of equipment losses.

<b>Corrective Actions</b>	<b>Current Status of Corrective Actions</b>
7.1. The Office of the Controller will complete the Underwriter Exposure Summary and receive an invoice for insurance coverage.	<b>Implemented</b>
7.2. Payment will be processed via Interdepartmental Charge Requisition.	<b>Implemented</b>
7.3. The Underwriter Exposure Summary will include a comprehensive inventory of Financial Management Information System Information Technology equipment, software, etc.	<b>Implemented</b>
<b>Audit Finding Resolved? Yes</b>	