INTERNAL AUDIT REPORT

Data Centers Assessment Follow-up

R-17-6

June 12, 2017

Contains sensitive security information that should not be publicized pursuant to Utah Code 63G-2-106 and 63G-2-305(12). Such information is also controlled under 49 CFR parts 15 and 1520 and may not be released without appropriate authorization. This information is highlighted in yellow in the internal Report and should be redacted from any public version of this Report.

Executive Summary

Introduction

A follow-up of the 2016 Data Centers Assessment Internal Audit has recently been completed. This report contains the results of the follow-up audit.

Objectives and Scope

The primary objective of the follow-up audit was to determine the status of management actions to address the findings reported in the 2016 audit report, reference R-16-3. The period of the follow-up audit was from October 1, 2016 through March 31, 2017.

The following areas were reviewed:

- Physical Security
- Environmental Control
- Data Center Administration

As the focus of the audit was on assessing progress with management actions to address the previously reported findings, controls that were evaluated as adequate and effective in 2016, were not tested and were assumed to be operating as they had at the time of the 2016 audit.

Audit Conclusion

Audit Report Rating*	
The overall rating has been determined based on the follow-up audit results. The audit revealed that physical security, environmental control, and data center administration risks had been largely addressed. The steps taken include the establishment of a disaster recovery site, improvements made to data center access procedures, and the identification of critical telecom closets. Some less significant risks remain that could be addressed by documenting the environmental risk assessments and clarifying responsibilities for both granting telecom closet access and removing access to external data centers. While this report details the results of the follow-up audit based on limited sample testing, the responsibility for the maintenance of an effective system of internal control and the prevention and detection of irregularities and fraud rests with management.	

*Rating is defined in Appendix 2

Internal Audit would like to thank the management and staff for their co-operation and assistance during the audit.

Table of Contents

APPENDIX 1

APPENDIX 1

1. Disaster Recovery Site

Finding	HIGH
UTA should have a disaster recovery site for its data center. An organization should have a disaster recovery site in place that can be used, in the case that the data center goes down, to recover backups and restore critical systems and data. Requisite hardware, connectivity, and the storage of backup files should align with the organizational disaster recovery plan. A disaster recovery site should also be located far enough away from the data center to limit its exposure to the same risks that comprise the data center's operations. Failure to have a disaster recovery site may result in UTA losing data and computer systems, shutting down of operations for longer than necessary, higher costs to obtain a site at the time of an emergency, and reputation damage. Audit procedures found that UTA does not currently have a disaster recovery site. However, it was also noted that IT identified the need for a disaster recovery site in 2015, began the process to identify an appropriate site and provider, and accounted for the additional expense in its 2016 budget. IT was in the process of writing a request for proposal and waiting for the 2015 carry-over capital budget at the time of this audit.	

Recommendation 16.3.1
The Deputy Chief – Information Systems Manager should secure or set-up a disaster recovery site that is sufficiently removed from the data center that it will not be impacted by the same events that might render the primary location inoperable.

Management Agreement	Owner	Target Completion Date
Yes	Deputy Chief – Information Systems Manager	August 31, 2016
The Deputy Chief – Information Systems Manager will continue the current procurement process to identify and contract with a third party to provide a suitable disaster recovery site for UTA by the end of August 2016.		

Final Status	Implemented
[redacted]	

Management Agreement	Owner	Target Completion Date
N/A	N/A	N/A
N/A		

APPENDIX 1

2. Environmental Controls

Finding	MEDIUM

UTA should ensure that telecom closets have adequate environmental controls. It is important to maintain a suitable environment within telecom closets for IT equipment to function under normal conditions. Additional controls should be in place to protect IT hardware and support its operation during abnormal events (e.g., loss of power, power surge, fire, etc.). Not all telecom closets are created equal in that some may house more critical or sensitive hardware than others. Consequently, the nature and extent of environmental controls needed for a telecom closet may vary. Organizations should have clear guidelines of what circumstances would require certain environmental controls.

Failure to have appropriate environmental controls in place may result in hardware damage, system failure, loss of data, and financial and reputational damage.

Audit procedures found that two (2) of the five (5) telecom closets inspected lacked adequate environmental controls. [redacted]

Recommendation 16.3.2

The Deputy Chief – Information Systems Manager should assess telecom closets to identify those housing hardware that require environmental controls and implement those controls as needed.

Management Agreement	Owner	Target Completion Date
Yes	Deputy Chief – Information Systems Manager	July 31, 2016

The Deputy Chief – Information Systems Manager will conduct a telecom closet assessment to identify environmental control needs and will oversee the implementation of the necessary controls. [redacted]

Final Status	LOW

Follow-up procedures revealed that a criticality assessment had been undertaken for telecom closets and additional controls had been implemented for select closets. However, no documented environmental risk assessment was created, including identified risks and the associated costs to address those identified remaining needs.

It is recommended that an environmental risk control exercise for telecom closets be documented.

APPENDIX 1

Management Agreement	Owner	Target Completion Date
Yes	IT Network Support Manager	12/31/2017
The Chief Safety, Security and Technology Officer or designee will perform a yearly risk assessment on UTA datacenter(s) and Telecom Closets. First assessment to be complete by end of year 2017.		

3. Data Center and Telecom Closets

Finding	HIGH

Access to UTA's data center and telecom closets should be restricted to personnel with job responsibilities requiring access. Entry points to facilities housing critical IT resources (IT facilities) should be secured to prevent unauthorized access. Additionally, a formal process should be in place for provisioning access to IT facilities. The process should require that:

- Requests for access to IT facilities are approved by a designated IT approver.
- IT periodically reviews individuals with access to IT facilities.
- Access is removed from individuals who no longer require access in timely manner.
- All approvals, reviews and terminations of access to IT facilities are documented.

Unauthorized access to the data center or telecom closets may result in hardware theft or damage and unauthorized access to or loss of data.

Recommendation 16.3.3
The Chief Safety and Security Officer should work with IT and Facilities to ensure that telecom closets are adequately secured.

Management Agreement	Owner	Target Completion Date
Yes	Chief Safety and Security Officer	September 30, 2016
The Chief Safety and Security Officer will work with IT and Facilities to ensure that telecom closets are adequately secured.		

APPENDIX 1

Final Status	Implemented
[redacted]	

Management Agreement	Owner	Target Completion Date
N/A	N/A	N/A
N/A		

Recommendation 16.3.4
The Deputy Chief – Information Systems Manager should work with Facilities to formalize the processes for provisioning access to the data center and telecom closets to ensure that IT reviews and approves access requests.

Management Agreement	Owner	Target Completion Date
Yes	Deputy Chief – Information Systems Manager	August 31, 2016
The Deputy Chief – Information Systems Manager will formalize the internal process for granting and removing personnel's access to the data center to ensure that only appropriate individuals are granted access [redacted] in a timely manner. The Deputy Chief – Information Systems Manager will work [redacted] to also control granting or removing access for employees needing access to the telecom closets. This will include [redacted] to review and approve requests for access to the telecom closets.		

Final Status	LOW
Follow-up procedures have shown that a formal process has been implemented and documented [redacted] for granting and removing personnel access to the third party data centers. However, further documentation is needed covering retrieval of third party provided access or identification cards that had been issued. In addition, follow-up procedures found that although oversight and required approvals for physical key access have been documented [redacted] It is possible that where such closets exist the requirement of appropriate IT approval for access is not understood or followed. [redacted]	

APPENDIX 1

[redacted]

It is recommended that the Technology Office Procedure [redacted] is expanded to include the requirement for the authorized approver retrieve any third party issued access or identification cards when access is revoked. Also, SOP [redacted] should be updated to include clarification of what constitutes a telecom room as well as who is authorized to approve access.

Lastly, the risk of unauthorized access to telecom closets should be documented and acknowledged by the appropriate level of management.

Management Agreement	Owner	Target Completion Date
Yes	IT Network Support Manager	12/31/2017

The Chief Safety and Security Officer or designee will update the Technology Office Procedure [redacted] with the required third party access removal procedure and what physical cards need to be collected upon access revocation due to termination, changes in job duties or disciplinary action.

Recommendation 16.3.5
The Deputy Chief – Information Systems Manager should establish a formal process for reviewing individuals' access to the data center and critical telecom closets to ensure that access is limited to only personnel whose responsibilities require that they have access to these facilities.

Management Agreement	Owner	Target Completion Date
Yes	Deputy Chief – Information Systems Manager	September 30, 2016

The Deputy Chief – Information Systems Manager will establish a process [redacted]

Final Status	**LOW**
Follow-up procedures showed that reviewing the individual's access for offsite data centers and critical telecom closets had been performed and documented. However, the Facilities' personnel access and requirement for approval has not been addressed.	

Management Agreement	Owner	Target Completion Date
Yes	IT Network Support Manager	12/31/2017

The Chief Safety, Security and Technology Officer or designee will investigate the possibility of auditing Facilities personnel and based on the findings add to the SOP [redacted]

APPENDIX 2

* REPORT RATING MATRICES

OVERALL REPORT RATING

The overall report ratings are defined as follows, applicable to the audit scope as defined

Descriptor	Guide
Fully effective	Controls are as good as realistically possible, both well-designed and operating as well as they can be.
Substantially effective	Controls are generally well designed and operating well but some improvement is possible in their design or operation.
Partially effective	Controls are well designed but are not operating that well. OR While the operation is diligent, it is clear that better controls could be devised.
Largely ineffective	There are significant gaps in the design or in the effective operation of controls – more could be done.
Totally ineffective	Virtually no credible controls relative to what could be done.

DETAILED FINDING PRIORITY RATING

Descriptor	Guide
High	Matters considered being fundamental to the maintenance of internal control or good corporate governance. These matters should be subject to agreed remedial action within three months.
Medium	Matters considered being important to the maintenance of internal control or good corporate governance. These matters should be subject to agreed remedial action within six months.
Low	Matters considered being of minor importance to the maintenance of internal control or good corporate governance or that represents an opportunity for improving the efficiency of existing processes. These matters should be subject to agreed remedial action and further evaluation within twelve months.
Implemented	Adequate and effective management action taken to address the finding noted in the audit report.

APPENDIX 3

DISTRIBUTION LIST			
Name	**For Action[1]**	**For Information**	**Reviewed prior to release**
President/CEO		*	*
General Counsel		*	
Chief Safety, Security and Technology Officer	*		*
IT Network Support Manager	*		*

[1]For Action indicates that a person is responsible, either directly or indirectly depending on their role in the process, for addressing an audit finding.