UTHealth®
The University of Texas
Health Science Center at Houston

Office of Auditing & Advisory Services

August 24, 2015

Report on General Controls Audit #15-201

We have completed our audit of general controls over the UCT data center. This audit was performed at the request of the UTHealth Audit Committee and was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing*.

BACKGROUND

Information technology (IT) general controls apply to all system components, processes, and data for a given organization or IT environment. The objectives of IT general controls are to ensure the proper development and implementation of applications, as well as the integrity of programs, data files, and computer applications. One of the most common IT general controls is physical security around a data center, including access, fire/flood measures, power safeguards, temperature/humidity monitoring, and physical configuration.

Data centers are centralized locations where computing and network equipment is concentrated for the purpose of collecting, storing, processing, distributing or allowing access to large amounts of data. In the early days of computers, a data center typically consisted of one large mainframe computer. As data processing needs have increased and equipment has become smaller and cheaper, multiple servers began to be networked together to increase processing power. Large numbers of these clustered servers and related equipment can be housed in a room, an entire building, or groups of buildings. Modern data centers have thousands of extremely powerful and small servers running continuously.

UTHealth currently maintains three data centers in the following locations; UCT, Medical School, and School of Public Health (SPH). The UCT and Medical School data centers are managed by Data Center Operations and Support Services (DCOS), while SPH is managed by IT personnel embedded within their organization.

The University of Texas Systemwide Policy 165 (UTS 165)

UTS 165 Standard 16, *Data Center Security*, requires that all information resources be physically protected based on risk and safeguards adopted to ensure appropriate granting, controlling, and monitoring of physical access. For data centers, physical access safeguards must incorporate procedures for:

(a) Protecting facilities in proportion to the criticality or importance of their function and the confidentiality of any information resources affected;
(b) Managing access cards, badges, and/or keys;
(c) Granting, changing, and/or removing physical access to facilities to reflect changes in an individual's role or employment status; and

(d) Controlling visitor and vendor physical access with procedures that incorporate advanced scheduling, logging, and documenting of visits; escorting while on premises; and restricting the unauthorized use of photographic and video devices while on premises.

Physical Security
The *Physical Security Policy* (ITPOL-010) applies to geographically restricted areas (GRAs), otherwise known as "data centers", and requires that access be physically restricted to those with a need to know. Numerous controls are required, including:

- Individuals without physical access authorization to enter a GRA must identify themselves using a UTHealth or other government-issued ID and sign a logbook maintained for the GRA. Persons without physical access authorization and that are unescorted by authorized personnel will not be admitted.
- Vendors are required to provide identification and proof of current employment via the means of a valid employee badge and, prior to granting access, the resource manager or their designee must verify the vendors' need for physical device access.
- Only person(s) who are granted physical access to GRAs are allowed to escort visitors and they must be monitored during their entire visit to the GRA.
- For GRAs, the independent temperature/humidity controlled environment must be fully supported by emergency power, perimeter walls must extend from the structural floor to the structural ceiling, and physical mechanisms must be in place to control site access.
- Access control lists must be maintained and reviewed semi-annually by the GRA Resource Owner or their designee, with evidence of review and resulting modifications maintained according to records management policies.
- Access logs must contain the names, date, and times visitors enter and leave the facility.
- All entry and exists must be monitored via video surveillance and electronically stored for future reference as required.
- Other requirements include self-closing and locked access doors, remotely-monitored security alarms, Uninterruptible Power Supply (UPS) adequate to supply 100% of system power for a 15-minute duration, fire detection and suppression system, and an adequately rated emergency power generator.

OBJECTIVES

The objective of this audit is to determine whether the general controls over the UCT data center are adequate and functioning as intended.

SCOPE AND METHODOLOGY

Through a review of physical access, fire and flood controls, power safeguards, temperature and humidity monitoring, and physical configuration, Auditing and Advisory Services (A&AS) performed an audit of the general controls over the UCT data center. The audit focused on the UCT data center as it is the central repository for UTHealth's mission critical information.

AUDIT RESULTS

Physical Access
A&AS conducted a walkthrough of the data center and adjacent rooms and verified the following:

- Badge access is required to enter the data center
- Data center lobby terminals are password-protected and locked when not in use
- The close-circuit television system (CCTV) is working properly, provides adequate coverage, and footage is archived for up to 90 days or to a certain memory limit
- The access door to the roof (used to access the generator and chillers) is properly secured

A&AS obtained evidence that data center access listings are regularly reviewed by the Senior Systems Administrator and verified that only authorized employees have access to data center badge entry doors. We verified that data center access request forms are properly approved by the Senior Systems Administrator and Chief Technology Officer. Additionally, we verified that the distribution of bypass and other manual entry keys to authorized employees is appropriate.

A&AS obtained the badge activity log from The University of Texas Police at Houston (UT Police) and verified that there were no unauthorized individuals that accessed the data center during the audit period. Additionally, we obtained the visitor log for the audit period and determined that it is not consistently completed by visitors. We also selected a random sample of 25 visitor entries and inquired about the appropriateness of each visitor with data center personnel. For three visitors, we could not determine whether access was appropriate.

Recommendation #1:

1a We recommend that a "Reason for Visit" field be added to the visitor log in order to document the appropriateness of the visit.

1b We recommend that operators be required to verify that the visitor log has captured all required information when a visitor is allowed access to the data center.

Management's Response 1a: We agree with the recommendation and will add the "Reason for Visit" field to the visitor log. Additionally, we will update our *Visitor Logging Policy* to reflect this change.

Responsible Party: Kevin Granhold
Implementation Date: September 30, 2015

Management's Response 1b: We agree with the recommendation and will require the operators to verify that the visitor log has captured all required information when a visitor is allowed access to the data center. Additionally, we will update our *Visitor Logging Policy* to reflect this change.

Responsible Party: Kevin Granhold
Implementation Date: September 30, 2015

When a badge access door is held open for more than 45 seconds or opened without a badge swipe, an alarm notification is automatically sent to UT Police, who will send an officer to investigate. A&AS confirmed with UT Police that no security incidents (alarm notifications other than false alarms) were noted during the audit period. Additionally, we conducted a total of six access breach tests and found that in two cases, UT Police did not receive an alarm notification.

Recommendation #2:

We recommend that DCOS work with UT Police to conduct a full test of all UCT data center badge entry doors to ensure that alarm notifications are working properly.

Management's Response: We agree with the recommendation and will work with UT Police to conduct a full test of all UCT data center badge entry doors to ensure that alarm notifications are working properly.

Responsible Party: Kevin Granhold
Implementation Date: November 30, 2015

Fire and Flood Controls

A&AS conducted a walkthrough of the data center (including adjoining rooms) and verified the following:

- Fire and heat detectors are installed in the data center and adjoining rooms
- Fire suppression systems are installed in the data center and adjoining rooms
- Leak sensors, water detectors, and floor drains are installed throughout the data center
- Fire extinguishers are located throughout the data center
- The data center is clean and free from obstructions
- No flammable supplies are present in the data center
- Cables in the data center are organized above rack or under flooring (with water-resistant sealant or cabling troughs)
- Medical supplies are clearly labeled and easily accessible in the operator room
- Flashlights are installed throughout the data center and operating correctly
- Abort buttons for the fire suppressions system (SAPPHIRE) are located in the operator room and at the entrance and exit to the data center

A&AS obtained the inspection reports for the fire suppression systems and fire extinguishers and verified that they are inspected on a regular basis. Additionally, we verified that the data center receives a deep cleaning on an annual basis.

Management was unable to provide evidence that data center employees attend fire safety training on a semi-annual basis.

Recommendation #3:

We recommend that attendance logs be used to document that DCOS personnel have attended semi-annual fire safety training.

Management's Response: We agree with the recommendation and will begin using attendance logs to document that DCOS personnel have attended semi-annual fire safety training. Additionally, we will develop and implement a *Data Center Fire Safety Training Policy* to reflect this change.

Responsible Party: Kevin Granhold
Implementation Date: November 30, 2015

Power Safeguards
According to the Telecommunications Industry Association's *Telecommunications Infrastructure Standard for Data Centers* (TIA-942), Tier 2 data centers (applicable to the UCT data center) should include a diesel-fired standby generator system and on-site fuel storage tanks that provide a minimum of 24 hours of generator operation. The use of a diesel generator is recommended due to the fast starting time, independence from gas utility companies, and certainty of operation time. A&AS noted that the backup generator for the UCT data center is powered by natural gas rather than diesel. While this increases the reliance on the utility supplier and creates uncertainty in regards to operation time, the risk is largely mitigated by the replication of mission critical information to the Guhn Road backup data center. However, certain functions such as telecommunications and network storage would be unavailable if the supply of natural gas is interrupted.

A&AS conducted a walkthrough of the UCT data center and verified that an emergency power-off switch (EPO) is available in the operator room (under a plastic cover behind the entry door) and that breakers are present in the electrical room; however, it was determined through discussions with DCOS personnel that the EPO is not currently configured to shut off all power to the data center. It is currently connected to only 6 of the 11 uninterruptable power supply (UPS) units and 5 of the 9 computer room air conditioning (CRAC) units.

Recommendation #4:
We recommend that the EPO switch be configured to include all UPS and CRAC units.

Management's Response: We agree with the recommendation and will configure the EPO switch to include all UPS and CRAC units.

Responsible Party: Kevin Granhold
Implementation Date: November 30, 2015

A&AS verified that the inspection and maintenance of UPS units, the generator, and transfer switches is performed on a regular basis. We obtained evidence that UPS self-tests occur on a biweekly basis. Additionally, we judgmentally selected a sample of UPSs and obtained the associated self-test issue log, noting no problems were logged.

A&AS observed a generator load test and obtained the generator run log as evidence that load tests are conducted on a weekly basis, with some exceptions for holidays and other technical issues.

Temperature and Humidity Controls
A&AS conducted a walkthrough of the UCT data center and verified that temperature and humidity sensors are installed throughout the facility. We also obtained screenshots from the monitoring software to verify that temperature and humidity settings (as well as alarm configurations) are set to the desired ranges.

A&AS verified that the inspection and maintenance of chillers, chiller pumps, air handling units, and CRAC units is performed on a regular basis. Additionally, we verified that air filters are regularly replaced during the quarterly air handling unit inspections.

Physical Layout

A&AS obtained the physical layout map of the UCT data center and verified that it is kept current. Additionally, we obtained the network port location map as evidence that the network ports are organized and the locations documented.

During the walkthrough conducted by A&AS, we randomly selected three server units and verified that the cables were labeled and color-coded by category as required by the *Datacenter Network Cable Color Standards* policy.

CONCLUSION

In our opinion, the controls over the UCT data center are generally appropriate and functioning as intended. Recommendations were made for improving data collection on the visitor log, conducting a full test of badge access doors to ensure proper alarm notifications, recording attendance of fire safety training, and configuring the EPO switch to include all UPS and CRAC units.

We would like to thank the DCOS staff and management who assisted us during our review.

Daniel G. Sherman, MBA, CPA, CIA
Assistant Vice President

DGS: BBS

cc: Audit Committee
Rick Miller
Kevin Granhold

Audit Manager: Brook Syers, CPA, CIA, CFE, CISA
Auditor Assi ned: Tammy Tran

Issue Date: September 2, 2015