



University Data Center

July 2024

Office of Internal Audits
UT Austin's Agents of Change



Executive Summary

University Data Center

Project Number: 24.038

Audit Objective

The objective of this audit was to evaluate the effectiveness of the physical and environmental safeguards at the University Data Center (UDC), including access controls, monitoring systems, emergency response plans, and environmental controls.

Conclusion

The UDC has established effective controls surrounding physical and environmental risks. There were no reportable issues, and the UDC has the following notable practices in place:

- Robust redundancies to allow for maintenance or replacement of equipment without disruption to ongoing operations.
- Strong controls over capacity and redundancy measures to absorb denial of service attacks.
- Detailed procedural documentation for maintaining and testing facilities and equipment that control the environmental systems, such as power supply, fire suppression, and cooling systems.

Audit Observations

No recommendations were provided.

Engagement Team¹

Mrs. Suzi Nelson, CPA, CIA, CISA, Senior Auditor
Mr. Paul Douglas, CISA, CCSFP, CDPSE, Partner, EAG
Mr. Michael Richmond, CISSP, CMMC-RP, Partner, EAG
Ms. Laura Walter, Senior Consultant, CISA, EAG

¹ This project was co-sourced with EAG Gulf Coast, LLC (EAG).



Conclusion

The UDC has established effective controls surrounding physical and environmental risks. There were no reportable issues, and the UDC has the following notable practices in place:

- Robust redundancies to allow for maintenance or replacement of equipment without disruption to ongoing operations.
- Strong controls over capacity and redundancy measures to absorb denial of service attacks.
- Detailed procedural documentation for maintaining and testing facilities and equipment that control the environmental systems, such as power supply, fire suppression, and cooling systems.

Table: Controls Assessment

Audit Objective	Controls Assessment
Evaluate the effectiveness of the physical and environmental safeguards at the University Data Center, including access controls, monitoring systems, emergency response plans, and environmental controls.	Effective
Breakdown by Area:	
Contracting and Asset Management	Effective
Logical and Physical Access	Effective
Emergency Response Plans	Effective
Physical and Environmental Controls	Effective
Availability of System Hardware	Effective
Networking and Encryption	Effective
Patch Management	Effective

Additional Consideration for Management

The Uptime Institute (Institute) maintains the leading data center Tier classification system used globally to measure data center performance. Tier III designation indicates that a data center has met stringent requirements for redundancy and infrastructure maintenance to ensure high availability and reliability. UDC’s attainment of this status could help achieve its goal of acquiring additional customers.

The UDC currently meets several of the Institute’s Tier III redundancy requirements related to availability. However, to better align with the criteria, the UDC needs a minimum 72-hour supply of on-site diesel fuel to sustain operations during extended outages and would also need an on-site water supply to sustain chillers. The UDC presently has 48 hours of on-site diesel



supply and has contracted with a vendor to provide additional diesel as needed. UDC also has an informal agreement with the executive director of Facilities Services to use the unit's water truck. To help achieve Tier III status, management should consider maintaining a 72-hour supply of on-site diesel and formally documenting the agreement with Facilities Services, including UDC's priority level for receiving water in the event of a disaster event.

Background

The UDC provides a secure, professionally managed data center to meet the growing information technology needs of researchers, colleges and schools, and administrative units at The University of Texas at Austin (UT Austin). The UDC team operates and manages UT Austin's data center and backup facilities, ensuring critical servers are available 24 hours a day. The facility has redundant power and cooling systems, redundant data center-class high-speed networking, and hardware firewall services managed by UDC Networking and Telecommunications.

The UDC also provides data center services to multiple external customers and has capacity to expand the number of both internal and external customers served.

Scope, Objectives, and Methodology

This audit was conducted in conformance with The Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*. Additionally, we conducted the audit in accordance with Generally Accepted Government Auditing Standards and meet the independence requirements for internal auditors. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions on our audit objectives.

The scope of this review included the UDC's current physical and environmental safeguards and operations. Key areas evaluated were:

- Contracting and Asset Management
- Logical and Physical Access
- Emergency Response Plans
- Physical and Environmental Controls
- Availability of System Hardware
- Networking and Encryption
- Patch Management

The specific audit objective and the methodology to achieve the objective are outlined in the table below.



Table: Objectives and Methodology

Audit Objective	Methodology
Evaluate the effectiveness of the physical and environmental safeguards at the UDC, including access controls, monitoring systems, emergency response plans, and environmental controls.	<ul style="list-style-type: none"> • Interviewed stakeholders to understand the design of controls for each control area. • Performed walkthroughs, inspected evidence, and performed controls testing to evaluate the effectiveness of each control area.

Criteria

- National Institute of Standards and Technology (NIST) Special Publication 800-209 and Special Publication 800-171 frameworks
- International Standard (ISO/IEC) 22337-1
- UT-IRUSP Standard 16: Data Center Security

The table below summarizes the relevant TAC 202 requirements covered during this audit.

Control Family	Control #	Control Name
Physical and Environmental Protections	PE-3	Physical Access Control
	PE-13	Fire Protection
	PE-14	Environmental Controls
Contingency Planning	CP-9	System Backup
	CP-10	System Recovery and Reconstitution
Personnel Security	PS-1	Policies and Procedures
	PS-4	Personnel Termination
Assessment, Authorization, And Monitoring	CA-7	Continuous Monitoring
Configuration Management	CM-1	Policies and Procedures
	CM-3	Configuration Change Control
	CM-5	Access Restrictions for Change



Report Submission

We appreciate the courtesy and cooperation extended throughout the audit.

Respectfully Submitted,

A handwritten signature in blue ink that reads "Sandy Jansen".

Sandy Jansen, CIA, CCSA, CRMA, Chief Audit Executive

Distribution

Dr. Jay C. Hartzell, President

Mr. Cole Campese, Vice President of Technology and Chief Information Officer

Mr. Cam Beasley, Chief Information Security Officer

Mr. Michael Martell, Director for Data Centers and Electronic Physical Security Systems

Mr. John Lovelace, Director of Networking and Telecommunications and Office of
Telecommunication Services

Ms. Christy Sobey, Director of Operations, Office of the President

The University of Texas at Austin Institutional Audit Committee

The University of Texas System Audit Office

Legislative Budget Board

Governor's Office

State Auditor's Office