INTERNAL AUDIT

Information Technology (IT) Physical and Environmental Security Audit
25-14

June 5, 2026

Table of Contents

Risk Rating Matrix

Descriptor	Guide
High	Major uncertainties are present. More is unknown than is known. No experience and/or data is available. Structure and resources are not established.
Moderate-high	Many uncertainties are present. Experience and/or data are limited. Structure and resources are incomplete, unproven and/or immature.
Moderate	Some uncertainties are present. As much is known as is unknown. Sufficient experience and data exist but may not be fully utilized. Structure and resources are adequate.
Low-moderate	Minor uncertainties are present. Strong experience and data exist. Structure and resources are well designed and supported.
Low	Little to no uncertainties remain. Significant experience and data exist and are fully utilized. Structure and resources are robust.

Distribution List

Title	For Action[1]	For Information	Reviewed prior to release
Audit Committee		*	
Executive Director		*	*
Chief Enterprise Strategy Officer	*	*	*
IT Director	*	*	*
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.

Executive Summary

Introduction

The Utah Transit Authority (UTA) Audit Committee directed the Internal Audit department (IA) to conduct an audit to verify that management has established governance over UTA's Information Technology Physical and Environmental Security. The Audit Committee approved an amendment to the 2025 Audit Plan that included this engagement on December 15, 2025.

Background and Overview

UTA's Information Technology (IT) Department supports nearly 3,000 employees by maintaining the organization's network infrastructure and servers as well as providing critical technology assets, including laptops, mobile phones, and touchpads. Effective physical and environmental security controls help protect these assets, support business operations, and reduce the risk of service disruptions, unauthorized access, equipment damage, and data loss.

UTA maintains technology infrastructure across multiple owned facilities, each of which contains data closets or data centers that house network and server equipment. In addition, the Company leases rack space for primary technology servers from two third-party providers: the University of Utah and Valor C3. These facilities host critical systems that support the UTA's daily operations and service delivery.

The IT Network Support Manager and Network Support staff are primarily responsible for implementing and maintaining physical and environmental security controls over IT infrastructure. Their responsibilities include the oversight of physical access to technology assets, monitoring environmental conditions, protecting equipment from physical threats, and supporting the secure operation of data centers and telecommunications spaces.

This audit evaluated the design and effectiveness of physical and environmental security controls over IT facilities, equipment, and supporting infrastructure. The review focused on measures intended to safeguard critical technology assets, restrict unauthorized access, and maintain reliable operating conditions across UTA's locations and third-party hosted environments.

Objectives and Scope

IA based the audit objectives and scope on the results of planning procedures that included discussions with management and assessments of risk and fraud risk. The topics for the audit were:

1. Oversight and Governance
2. Design and Implementation of Physical Security
3. Design and Implementation of Environmental Security

IA set the audit period as January 1, 2025, through February 28, 2026.

Executive Summary

1. **Governance**
   UTA has established governance structures and assigned responsibilities for overseeing physical and environmental security within the IT environment. The IT Network Support Manager and Network Support staff are responsible for administering controls that protect critical technology infrastructure and assets. The audit evaluated the policies, procedures, roles, and oversight mechanisms that support the management of physical and environmental security risks across UTA-owned facilities and third-party hosted environments.

2. **Design and Implementation of Physical Security**
   UTA maintains physical security controls designed to protect technology assets located in data centers, data closets, and other restricted IT areas. These controls include measures to restrict unauthorized access to critical infrastructure, safeguard IT equipment, and support the security of facilities that house network and server resources. The audit reviewed the design and implementation of physical access controls across UTA locations and at third-party hosting facilities operated by the University of Utah and Valor C3.

3. **Design and Implementation of Physical Security**
   UTA has implemented environmental security measures intended to maintain appropriate operating conditions for critical technology infrastructure and reduce the risk of service disruptions caused by environmental hazards. These controls include monitoring and protective measures for equipment located in data centers and telecommunications spaces. The audit assessed the design and implementation of environmental safeguards supporting the availability, reliability, and protection of IT systems and infrastructure.

Finding 25-14-01 Resolve access issues for certain data critical areas — Risk Level: Moderate

Criteria

ISACA standards state that identification badges (and other types of identification tokens) are used as a means of identifying individuals, associating access authority with the identified person, and controlling access through integration with physical access devices.

Condition

Management discovered that some employees who don't need access have access to some of the doors within UTA's facilities for restricted areas. The vendor acknowledged that there are multiple naming issues with the portals and readers that are causing this issue.

Cause

Management and the vendor did not maintain an accurate and standardized naming convention for access control portals and readers within the physical access management system. As a result, access permissions were assigned incorrectly, granting employees access to restricted areas that was not required for their job responsibilities.

Effect

Unauthorized or unnecessary access to restricted areas increases the risk of physical security breaches, unauthorized exposure to sensitive assets or information, and noncompliance with established access control requirements. Inaccurate access assignments may also impair management's ability to effectively monitor, review, and enforce physical access restrictions.

Recommendation

1. Management should work with the vendor to correct portal and reader naming inconsistencies and validate that all access control devices are accurately identified within the system.
2. Management should perform a comprehensive review of employee access rights and remove access privileges that are not supported by business or operational requirements.
3. Management should establish and enforce standardized naming conventions and change management procedures for access control devices to ensure accurate access provisioning and ongoing system integrity.
4. Management should implement periodic access reviews to verify that physical access privileges remain appropriate and aligned with employees' current job responsibilities and the principle of least privilege.

Management Response and Action Plan:

Management Response and Action Plan:
Management concurs with the finding. Access to data centers, data closets, and other critical IT areas must be governed as an enterprise risk control, not only as a technical or departmental process. While IT is responsible for supporting and administering many of these controls, multiple groups may have a legitimate business need to access these areas, including Facilities, Security, vendors, contractors, and certain operational staff.

Management will develop and implement a formal documentation governing access to critical IT areas. The policy will define access eligibility, approval authority, business justification requirements, emergency access expectations, vendor and contractor access requirements, documentation standards, and periodic access review expectations. This documentation will provide the governance and authority needed to support consistent enforcement of related work instructions across departments.

Management will also work with the access control vendor to identify the ability to improve and correct portal and reader naming inconsistencies and validate that access control devices are accurately identified in the system. Once the system information is corrected, management will review current access to restricted IT areas and revoke access that is not supported by job responsibilities, operational need, or an approved exception.

To sustain the control environment, management will establish standardized naming conventions, set expectations for change control for access control devices, and conduct recurring access reviews. These actions will help ensure physical access remains accurate, appropriate, and aligned with the principle of least privilege

Responsible:
IT Director

Target Completion Date:
6/03/2027

Finding 25-14-02 Enterprise-wide emergency response plan for critical IT areas Risk Level: Moderate

Criteria
ISACA standards state that an emergency response plan should exist that outlines how the enterprise responds to and recovers from emergencies, disasters and other significant incidents impacting its information-processing facilities.

The plan should be:

- Approved by senior management
- Clearly define key roles and responsibilities for emergency operations
- Covers types of emergency situations and significant events that are most likely to affect the facility.
- Is current and relevant (i.e. addresses existing and potential threats at the site/facility).

Condition
Management acknowledged that current "back to paper" plans are outdated and in need of updating.

Cause
Management has not implemented a formal process to periodically review, update, and approve emergency response documentation. Consequently, the existing "back to paper" plans no longer reflect current business operations, personnel responsibilities, systems, or potential emergency scenarios.

Effect
The organization may not respond to or recover from a disruption in a timely and effective manner due to outdated emergency procedures. This increases the risk of operational disruption, extended downtime, unclear roles and responsibilities during an emergency, and non-compliance with established standards and leading practices.

Recommendation

1. Management should review, update, and formally approve emergency response plans to ensure they remain current and effective. The revised plans should clearly define roles and responsibilities, address relevant emergency scenarios, reflect current business operations and technology environments.
2. Management should also develop a process to include periodic review and testing to maintain readiness and compliance with organizational requirements and industry standards.

Management Response and Action Plan:
Management would like to clarify that the Emergency response plan does not have the same purpose as the back-to-paper plans. This management response will address the outdated paper-based plans in relation to disaster recovery.

Management will update the "back to paper" procedures to reflect the current operating environment and likely disruption scenarios. The updated plans will define roles and responsibilities, communication expectations, escalation steps, manual workarounds, recovery priorities, and coordination requirements for events that impact critical IT areas or the business processes that depend on them.

Management will also establish clear ownership, formal leadership approval, periodic review, and testing expectations. This will help ensure the plans remain current, actionable, and understood by the teams that may need to execute them during an incident.

These actions are intended to strengthen UTA's ability to respond to disruptions, reduce avoidable downtime, and support continuity of operations when critical IT areas or supporting infrastructure are impacted.

Responsible:
IT Director

Target Completion Date:
6/03/2027

Finding 25-14-03 Update contract with the U of U to current standards Risk Level: Low

Criteria
ISACA standards state that the enterprise should include physical and environmental security requirements in contracts with third parties to protect against or minimize the impact of losses attributable to third-party services or personnel. This includes the enterprise's physical and environmental security requirements are contractually cascaded to the service providers (e.g., personnel screening, personnel training and awareness).

Condition
UTA currently contracts with the University of Utah (U of U) and Valor C3 to lease server space at existing data centers. In reviewing the contracts IA noted that the Master Agreement with the U of U was outdated having been first executed in 2011. Additionally, the agreement does not contain language addressing the following areas:

- Incentivizes or obligates the service provider to perform/meet set service expectations.
- Allows the organizations to assess the performance of service providers, e.g., periodic reporting and right to audit, third-party assurance, security certification, performance appraisal, compliance, etc.

Cause
Management did not establish or consistently execute a formal contract governance and review process to ensure that third-party agreements remain current and incorporate required security, performance, monitoring, and compliance provisions. Consequently, the agreement with the University of Utah was not periodically reassessed and updated to reflect evolving business, operational, and security requirements.

Effect

Outdated and incomplete contractual provisions limit UTA's ability to hold service providers accountable for meeting defined service and security expectations. The absence of performance measurements, reporting, audit, and assurance requirements reduces management's visibility into the effectiveness of third-party controls and increases the risk that security, compliance, or operational issues may go undetected or unresolved. This may also expose UTA to service disruptions, inadequate protection of critical infrastructure, and potential noncompliance with established governance and security standards.

Recommendation

1. Management should review and update the agreement with the University of Utah to incorporate current business, operational, physical security, and information security requirements, including clearly defined service expectations and responsibilities.
2. Management should ensure that all data center and third-party hosting agreements include measurable service level requirements, performance metrics, and provisions that establish accountability for service delivery and security obligations.
3. Management should incorporate contractual rights to monitor and assess service provider performance, including periodic reporting requirements, right-to-audit clauses, independent assurance reports, security certifications, compliance attestations, and other relevant oversight mechanisms.
4. Management should establish a formal third-party contract management process that requires periodic reviews of vendor agreements to verify that contractual terms remain current, address applicable risks, and align with organizational policies, regulatory requirements, and industry standards.

Management Response and Action Plan:

The University of Utah agreement supports critical technology infrastructure and should be reviewed from contract governance and vendor risk management perspectives.

Management will coordinate with Procurement, Legal, IT leadership, and other relevant stakeholders to review the existing University of Utah and any other data center and third-party hosting agreement(s) and determine the appropriate path for updating, amending, or replacing them at the next renewal opportunity.

Management will not establish a formal third-party vendor contract management process because UTA is standing up a contract management department to oversee this function.

Responsible:

IT Director

Target Completion Date:

6/03/2027