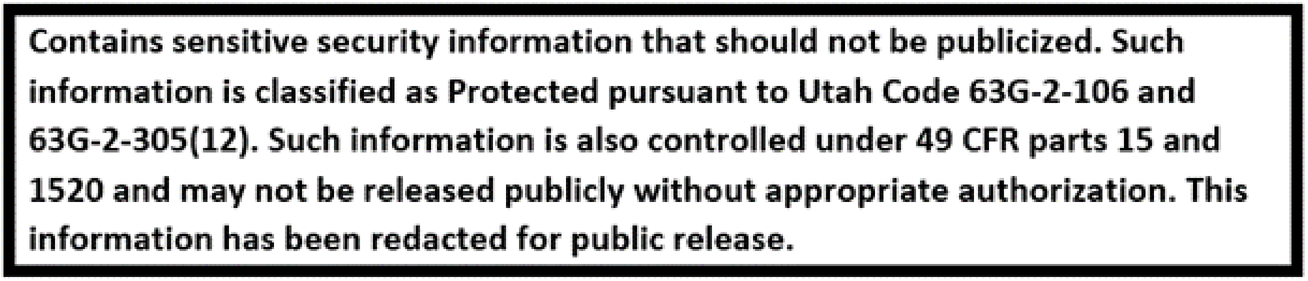
INTERNAL AUDIT

Sensitive Data Access Audit

R-19-05

October 19, 2021



Contains sensitive security information that should not be publicized. Such information is classified as Protected 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 publicly without appropriate authorization. This information has been redacted for public release.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

Table of Contents

Rating Matrix

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.

Distribution List

Title	For Action[1]	For Information	Reviewed prior to release
Executive Director		*	*
Chief Enterprise Strategy Officer		*	
Chief People Officer		*	
Information Technology Director		*	
Information Security Manager		*	
Records 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

In conjunction with the Audit Committee, Internal Audit (IA) developed a risk-based annual audit plan. This audit was conducted in accordance with the International Standards for the Professional Practice of Internal Audit, published by the Institute for Internal Auditors (IIA).

IA was directed by the Audit Committee to perform an audit to determine if controls over access to sensitive data are designed adequately and operating effectively to ensure compliance with federal regulations, state laws, and internal policies and procedures as well as to support the achievement of management objectives.

Background and Overview

The Director of Information Technology, Dan Harmuth, provided a functional overview of UTAs applications and data access to add context to this report. Please note that all of the statements made are assertions by the IT Director and were not assessed by Internal Audit.

UTA Information Technology (IT) is the custodian of data rights, as authorized by executive, department, and section managers, to UTA employees who need to access data and applications to do their jobs. Technology's goal is to protect and limit access to only those staff members that need access to data in order to perform their assigned task.

The scope of UTA in-house applications and data access is extremely large. UTA Technology supports:

- In excess of 85 applications (~29 COTS/SaaS, ~56 custom)
- Running on 721 databases (Production, development, test), using 33 database servers
- Holding 18.6 terabytes of application data (1 terabyte = 1,000 GB, iPhone = 64 GB)
- User and Shared Network Drives
- Total SAN (Storage Area Network) storage is ~630 TB of data

The IT Department aligns with The National Institute of Standards and Technology (NIST) which means that the IT Department utilizes NIST 800-100 Information Security as recommendations and suggestions in forming how it can provide information security at UTA with current resources. It is understood that NIST requires an enormous amount of resources that a public transportation agency would not be able to have for the level of security risk compared to other State or Federal agencies or private organizations, so directly measuring UTA against NIST is not applicable.

Objectives and Scope

The period of the preliminary assessment was October 1, 2018 through September 30, 2019 with the Preliminary Assessment report issued on June 18, 2019. The audit fieldwork commenced on August 10, 2021 and concluded on October 18, 2021.

The primary areas of focus were:

- Business data governance
- Business data protection and classification
- Active directory, as related to data access
- Access to sensitive applications and databases
- Software as a service (where related to sensitive data)

Summary

In general, the audit showed that the processes, practices, and procedures used to manage access to sensitive data are adequate. Appropriate controls are in place to identify, assess, and mitigate the risk associated with access to sensitive data.

The key findings identified in the Preliminary Assessment have been adequately addressed and resolved.

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

ATTACHMENT A: Details of Findings

Finding R-19-05-01 Governance — Resolved

Preliminary Assessment Condition Summary:

- IA reviewed 17 UTA policies or procedures relating to the access, security, and maintenance of sensitive data, of which, 12 listed the last review date prior to 2019, including 2 policies with the last review date in 2015.
- [redacted]

Audit Condition Detail - Remediated

IT Management has assigned a staff member the responsibility to review and update department governing documents on an annual basis and has implemented a new process requiring staff to document the acknowledgement of policies, procedures, and Management directives. The department also has centralized all governing documents to ensure staff is able to locate needed guidance.

Criteria:

- The IT Department uses The National Institute of Standards and Technology (NIST) as a general informational guide in developing practices. NIST 800-100 Information Security (special publication handbook) defines information security governance as the process of establishing and maintaining a framework, and supporting management structure and processes, to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk.
- UTA Policy 2.1.12 Information Technology Governance, dated 7/28/17, included assignment of ownership and responsibility for technology and applications as well as individuals and groups.

Inherent Risk:

[redacted]

Recommendations:

IA has determined the identified risk has been mitigated. No further action is required.

Audit Finding R-19-05-02 Department Governance Resolved

Preliminary Assessment Condition Summary:

[redacted]

Audit Condition Detail - Remediated

[redacted]

IT Management has assigned a staff member the responsibility to review and update department governing documents on an annual basis and has implemented a new process requiring staff to document the acknowledgement of policies, procedures, and Management directives. The department also has centralized all governing documents to ensure staff is able to locate needed guidance.

Criteria:

- The IT Department uses the National Institute of Standards and Technology (NIST) as a general informational guide in developing practices. NIST 800-100 Information Security (special publication handbook) defines Information security governance as the process of establishing and maintaining a framework and supporting management structure and processes to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk.
- UTA Policy 2.1.12 Information Technology Governance, dated 7/28/17, included assignment of ownership and responsibility for technology and applications as well as individuals and groups.
- The purpose of IT Department policy 6.0.3 Vulnerability Management Policy, dated 6/10/19, is to grant authorization to the Senior Information Security Administrator (SISA), or designee, to conduct Security Audits, consisting of probes, vulnerability assessments, and penetration tests.
- IT Department SOP 5.1.5 Information Security Incident Response Procedure gives detailed information on what to do in the event of a security breach dated 3/8/2018.

Inherent Risk:

[redacted]

[redacted]

[redacted]

Recommendations:
IA has determined the identified risk has been resolved. No further action is required.

Audit Finding R-19-05-03 Data Security Resolved

Preliminary Assessment Condition Summary:

- UTA developers had unmonitored administrative access to production databases instead of Read-Only access.
- The SISA's role included both the responsibilities for the administration and monitoring of security systems as well as developing a security policy, which created segregation of duties.

Audit Condition Detail- Remediated:

- Employees with both developer and administrative access to production databases have been assigned two different access credentials, which provides a clear audit trail of activities. Additionally, a third-party software monitors activities and alerts management when changes are made.
- IT department policies are reviewed and approved by IT Director before implementation. The SISA does not have the authority to administer policy.

Criteria:
The IT Department uses with the National Institute of Standards and Technology (NIST) as a general information guide when developing best practices.

- NIST 800-53: CM-5(5)(a) Access Restrictions for Change/ Limit Production/ Operational Privileges. Limiting privileges to change information system components with respect to operational systems is necessary because changes to a particular information system component may have far-reaching effects on mission/business processes supported by the system where the component resides. The complex, many-to-many relationships between systems and mission/business processes are in some cases, unknown to developers.
- NIST AC-5 Separation of Duties. Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, network administration, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions.

Inherent Risk:

- [redacted]
- [redacted]

Recommendations:
Previously identified risk has been mitigated. No further action required.

Audit Finding R-19-05-04 User Access Resolved

Preliminary Assessment Condition Summary:
IA observed and noted the following conditions regarding user access to sensitive data:

- The policy that assigned responsibility to a department to monitor user, service, and contractor accounts that access UTAs sensitive data is vague and unclear.
- [redacted]

Audit Condition Detail - Remediated:

- Department 1.03 Technology Access Control SOP has been updated to better define data ownership and user responsibilities.
- Internal audit conducted a review of 509 transferred employees, all employees had appropriate access.

Criteria:

- IT Department policy 1.0.5 Access controls are designed to minimize potential risk to the Utah Transit Authority (UTA) resulting from unauthorized use of Technology Resources and to preserve and protect the confidentiality, integrity, and availability of the UTA's networks, systems and applications.
- The process includes a monthly report of transfers generated and emailed to the JDE ERP Developer to verify transfers have been reassigned a group.

Inherent Risk:

- [redacted]

Recommendations:
The risk of inappropriate access for transferred employees has been resolved. No further action required.