

Stephen F. Austin State University

IT Asset Management Audit

As of October 31, 2023

Audit Report 24-102



Department of Audit Services

**Jane Ann Bridges, CPA, CIA, CFE, Chief Audit Executive
Box 6121, SFA Station
Nacogdoches, Texas 75962
Phone 936-468-5204
Email bridgesja1@sfasu.edu**

TABLE OF CONTENTS

EXECUTIVE SUMMARY 2
 AUDIT OBJECTIVES..... 2
 SCOPE..... 2
 SUMMARY OF AUDIT RESULTS 2
 ACKNOWLEDGMENTS..... 2
DETAILS OF AUDIT 3
 BACKGROUND..... 3
 AUDIT OBJECTIVE, SCOPE, AND METHODOLOGY..... 3
DETAILS OF AUDIT OBSERVATIONS 5
APPENDIX 1 OBSERVATION RATINGS 7

EXECUTIVE SUMMARY

The Department of Audit Services has completed an audit of Information Technology Asset Management (ITAM). As of October 31, 2023, the University had 11,508 IT assets on the University's property records valued at \$26,170,075.53.

AUDIT OBJECTIVES

The audit objectives were to gain assurance for the following:

- The University had a complete and accurate inventory of IT assets.
- IT assets were efficiently and effectively established, utilized, and managed to support the University or department/unit mission.
- The University was in compliance with applicable Texas Administrative Code §202.76 security control standards.

SCOPE

The audit scope included University IT assets as of October 31, 2023.

SUMMARY OF AUDIT RESULTS

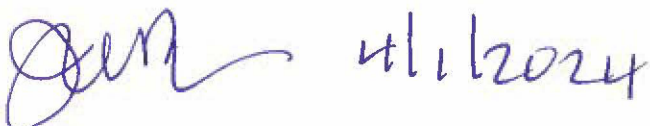
We found that the University did not have a complete and accurate inventory of IT assets and some IT assets were not being efficiently and effectively established, utilized, and/or managed. In addition, the University partially conforms with the Texas Administrative Code §202.76 security control standards specifically relating to IT asset management. While performing our audit, we noted an opportunity to strengthen controls, enhance compliance, or improve processes. Additional details can be found in *Details of Audit Observations*.

Observation	Rating
1 – IT Asset Management – University does not have a fully developed and formalized ITAM program.	High

* See Appendix 1 for Observation Rating descriptions

ACKNOWLEDGMENTS

We appreciate the assistance provided to us during our audit by the Department of Information Technology Services.



Jane Ann Bridges, CPA, CIA, CFE
Chief Audit Executive
Stephen F. Austin State University

DETAILS OF AUDIT

BACKGROUND

The Department of Audit Services has completed an audit of ITAM. The Department of Information Technology Services (ITS) maintains an internal ITS Policy Handbook, which was modeled on the Texas Department of Information Resources (DIR) Security Control Catalog framework. DIR Security Control CM-8, *System Component Inventory*, requires an organization to develop and document an inventory of system components that accurately reflects the system, includes all components within the system, does not include duplicate accounting of components or components assigned to any other system, is at the level of granularity deemed necessary for tracking and reporting, and identify specific information to achieve system component accountability. In addition, this control requires that an organization review and update the system component inventory on a defined frequency.

ITS Policy 14.1.7, *IT Configuration Management Policy*, requires the creation and periodic review of a list of university hardware and software assets. In addition, ITS Policy 14.1.7 assigns this IT asset management responsibility to the system owners as well as the security operations staff and gives the Chief Information Security Officer decision and delegation authority for the program.

IT assets, for purposes of this audit, are comprised of the following components:

- Capital Assets - IT items valued \$5,000 or more with a useful life greater than one year.
- Controlled Assets as defined by the State* - IT items valued between \$500 and \$5,000, specifically TVs, computers, servers, laptops, smartphones, tablets, other handheld devices, and drones.
- Controlled Assets as defined by the University* - IT items valued up to \$5,000, specifically computers, servers, laptops, tablets, printers (greater than \$500), and drones.
- Uncontrolled Assets – IT items that do not meet the criteria above but are relevant to IT asset management and the information security posture for the University (i.e., printers less than \$500).

Capital, State-Defined Controlled Assets, and University-Defined Controlled Assets are required to be recorded in the University property records*.

**Per the University's Property Manual*

As of October 31, 2023, the University had 11,508 IT assets on the University's property records valued at \$26,170,075.53.

AUDIT OBJECTIVE, SCOPE, AND METHODOLOGY

The audit objectives were to gain assurance for the following: the University had a complete and accurate inventory of IT assets; IT assets were efficiently and effectively established, utilized, and managed to support the University or department/unit mission; and the University was in

compliance with applicable Texas Administrative Code §202.76 security control standards. The audit scope included University IT assets as of October 31, 2023.

We performed our audit in accordance with the *International Standards for the Professional Practice of Internal Auditing* and *Generally Accepted Government Auditing Standards (GAGAS)*. The 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 findings and conclusions based on our audit objectives. The Department of Audit Services is independent per both standards for internal auditors.

The audit methodology consisted of performing a risk assessment; reviewing applicable policies, procedures, laws, and best practices; assessing internal controls; interviewing appropriate University personnel; testing for existence and compliance; reviewing supporting documentation; evaluating opportunities for fraud to occur; and performing other procedures as deemed necessary.

The audit criteria included:

- University of Texas System (UTS) policies;
- University procedures;
- Texas Administrative Code §202.76, Department of Information Resources Security Control Standards, specifically, control families Program Management (PM), Configuration Management (CM), Media Protection (MP), and Physical and Environmental Protections (PE);
- University Information Technology Services Policy Handbook;
- Other sound higher education IT guidelines and practices.

DETAILS OF AUDIT OBSERVATIONS

Observation 1: IT Asset Management

Background: DIR Security Control Standard PM-5, *System Inventory*, requires state agencies to “develop and update an inventory of organization systems.” DIR Security Control Standard CM-8, *System Component Inventory*, also requires an inventory of system components that accurately reflects the system, includes all components within the system, does not include duplicate accounting of components or components assigned to any other system, and is at the level of granularity deemed necessary for tracking and reporting. ITS Policy 14.1.7, *IT Configuration Management*, states, “The ISO shall create and periodically review a list of university hardware and software assets.” In addition, ITS Policy 14.1.7 states the ISO shall “monitor systems for security baselines and policy compliance.” ITS Policy 14.1.2, *Baseline Configuration*, states that the university will “develop and maintain a University-defined list of software programs authorized to execute on University Information Systems” and “employ a deny-all, permit-by-exception authorization policy to identify software allowed to execute on University Information Systems”.

Observation: The University does not have a fully developed and formalized IT asset management program. While performing our audit procedures, we noted the following:

- The University does not define IT assets and has not determined which IT assets should be included in the ITAM program.
- The University does not have a complete and accurate listing of University-defined IT assets as evidenced by a large number of desktops not on the IT hardware inventory.
- The hardware inventory provided did not contain key information such as location, serial number, asset owner, and a consistent asset naming convention.
- IT asset inventories have not been reviewed by management on a regular basis.
- A deny-all process for unauthorized software is not in place.
- During our detailed testing, we noted the following:
 - 6 of 20 (30%) IT assets selected for review were inoperable or not imaged despite being listed as “in use” in the property records.
 - 9 of 14 (64%) IT assets reviewed were using an outdated version of antivirus.
 - 3 of 14 (21%) IT assets reviewed had unauthorized software installed.

Observation Rating: High

Recommendation: The University should continue to develop and formalize the ITAM program in coordination with the revised UTS Policy 165, *Information Resources Use and Security Policy*, to ensure compliance with UTS policy, State guidance, and internal procedures.

Management Response: ITS will continue to develop and formalize the ITAM program to ensure compliance with UTS policy, State guidance, and internal procedures in a phased approach.

Responsible Party: Chief Information Officer

Implementation Date: March 31, 2025

APPENDIX 1 OBSERVATION RATINGS

Audit Services uses professional judgment to rate the audit observations identified in audit reports. The audit observation ratings are determined based on the risk or effect of the issues in relation to the audit objective(s), along with other factors. These factors include, but are not limited to, financial impact; potential failure to meet area/program/function objectives; level of compliance with laws, regulations, and other requirements or criteria; adequacy of the design of control activities and information system activities; level of potential fraud, waste, or abuse; control environment; history of audit issues; and other pertinent factors.

Rating	Description
Low	The audit observation does not present significant risks or issues that could negatively impact the University in the area/program/function audited. Action is needed to address the audit observation.
Medium	The audit observation presents risks or issues that if not addressed could moderately impact the University in the area/program/function audited. Action is needed to address the audit observation and reduce risks to a more desirable level.
High	The audit observation presents risks or issues that if not addressed could substantially impact the University in the area/program/function audited. Prompt action is needed to address the audit observation and reduce risks to a more desirable level.
Priority	The audit observation presents risks or issues that if not addressed could critically impact the University in the area/program/function audited. Immediate action is needed to address the audit observation and reduce risks to a more desirable level.

Other less significant observations may be shared verbally with management during the audit or at a concluding meeting.