INTERNAL AUDIT

Information Technology General Controls

Follow-up Report

R-21-05

February 18, 2025

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		*	
Information Technology Director		*	
Information Security Manager		*	
Enterprise Systems 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 information technology general controls 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.

IA completed the preliminary assessment phase with a report dated March 9, 2022 and completed an audit phase with a report dated March 6, 2023. IA completed final follow-up work on February 5, 2025.

Background and Overview

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

Objectives and Scope

Audit Phase

The time period reviewed was April 1, 2022, through November 30, 2022. The primary areas of focus for the preliminary assessment were:

- Governance
- Security Management
- Change Management
- Data Management
- Business Continuity
- Third-party service providers

IT topics are by nature complex and require a high level of expertise and experience to understand and apply. While Internal Audit has an understanding of IT topics and IT general controls, we lack the specific expertise to offer assurance over highly technical areas. This engagement should be not understood as a general assessment and not providing an depth, technical look at the IT control environment.

Follow-up Phase

IA limited the objectives and scope of the follow-up phase to determining the status of finding R-21-05-02, which finding recommended that IT adopt a framework of standards for information technology.

Summary

Audit Phase

Internal Audit reviewed, without exception, the following:

- IT has implemented a software that assists with threat detection and response.
- has installed a software that will track compliance with established standards.
- IT's governance within the organization is well established by policy and documentation.
- Rules for system user passwords are enforced and effective.
- Active Directory control is effectively managed. Timely communication from departments who hire contractors is needed, but this is not a reportable issue.
- Internal access to servers is limited to authorized employees.
- IT enforces installation of anti-virus software on user computers.
- Software patches are addressed and implemented.
- IT works closely with the Records department to implement data retention strategy.
- Data backups occur at regular intervals. Tests of backup data are performed monthly.
- IT provides UTA management with regular reports on cyber security vulnerabilities.
- IT maintains a business continuity and disaster recovery plan.

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

Follow-up Phase

IT provided evidence that a third-party, Optiv, completed an assessment and analysis of UTA's compliance with the National Institute of Standards and Technology Cybersecurity Framework. The report itself is evidence that IT has adopted NIST and satisfied finding R-21-05-02. IA has closed all findings from the initial audit report.

ATTACHMENT A: Status of Preliminary Assessment Recommendations

Finding R-21-05-01 Data Access Separation of Duties	High

Preliminary Assessment Condition Summary:
SOD helps protect the company against fraud by ensuring that any one user does not have access to applications that can be used to circumvent an approval process. Internal Audit attempted to prepare a detailed review of SOD within the JD Edwards environment. This review noted that the IT department does not maintain a data dictionary defining the functionality of objects.

The IT department relies on the Data Owners reviewing user access to determine if there are conflict of duties. However, without a data dictionary, or "key", to use to determine the functionality of objects, the reviewer cannot adequately determine if a user's access rights present a conflict.

Criteria:
UTA Department of Information Technology No. 1.0.5 Access Control Policy states:

> *III. The term "Authorized User" or "User" means any person who is authorized to use a specific Technology Resource. Authorization may be based on job title, job roles, job responsibility or other methods of access control. Authorization will be determined by the Department of Information Technology Supervisor in charge of the system or application, or designee, in consultation with the data owner.*
>
> *IV.C. Segregation of Duties*
> *1. Access to Technology Resources will only be provided to Authorized Users based on business requirements, job function, and/or responsibilities.*
> *2. All Authorized Users of Sensitive Data will have the appropriate authorization granted to them by the owner and/or system administrator of the Sensitive Data.*
> *3. Authorized parties granting access to Users must document the specific privileges.*
>
> *IV.D. User and Administrative Access*
> *4. All privileged access by data or system administrators will be reviewed no less than every 6 months by appropriate administrator and validated by the SISA.*

UTA Agency SOP No. AGCY01.03 Technology Access Control Standard Operating Procedure states:

> *2. "Separation of Controls and Duties" is an internal control designed to prevent damage, fraud, and error by ensuring that at least two individuals are responsible for separate parts of any sensitive task. An example would be by disseminating the duties and associated privileges for a specific business process among multiple users.*
>
> *2.A.2. Separation of Controls and Duties*
> *Authorization to a resource will rely upon feedback from the system, application or data owners, and the Department of Information Technology, utilizing job title, job roles, job responsibility, or other access control methods.*
>
> *2.B.1. Authorized User Account and Access Management*

Each Department will define data access roles that support segregation of duties in order to reduce unauthorized data access and use.

UTA Corporate Policy No. 1.1.23 Information Security Policy states:

IV.A.7. Individual Accountability

The Technology Department has the right to limit User's access to Technology Resources based on best practices, least privilege or contractual, compliance or regulatory requirements.

Cause:
Not determined.

Inherent Risk:
Users access rights may grant them the ability to circumvent established approval process, allowing them to perform tasks outside their responsibilities and authority. This access can lead to undetected fraud, waste, mistakes, or abuse.

Recommendations:
1. IA recommends the Enterprise Applications department prepare a list specifying the function of each object in the JD Edwards environment and provide it to the Data Owners that review user access.
2. IA recommends the IT department develop an alert to detect when conflicting duties are assigned to a user and require an approval before assignment of conflicting duties takes effect.

Management Response and Action Plan:
Creating a data dictionary of all objects is the JD Edwards environment would result in millions of records and would be unmanageable. It would also be a never-ending task and any benefit of a Data Dictionary would be negated by the effort in keeping it current.

The Enterprise Applications Department believes that many of Internal Audit's objectives listed above can be achieved by creating a Sensitive Objects list and having access to these objects approved by the JDE Superusers that are all subject matter experts in their respective functional areas.

Furthermore, the Enterprise Applications Team will research options to determine if a system alert can be proactively created that will provide a notification in the event a conflict-of-interest duty is created.

Target Completion Date:
March 31, 2023

Current Status – Audit Phase:
Closed.

Management determined that it would be infeasible to create a comprehensive Sensitive Objects list for the JD Edwards application. This is because of the high number (potentially thousands) of objects, and they are not subject matter experts on what duties constitute a conflict.

Management relies on departments to manage conflicting duties through job and task assignment. To assist management with identification of potentially conflicting object access, management sends a quarterly report to department management listing objects and who has access and what access they have. Management can then review the list to determine if access is appropriate for current circumstances.

From IT's perspective, they have appropriately mitigated the risk. Separation of duties must be considered a departmental, end-user issue.

Finding R-21-05-02 Security Standards — Medium

Preliminary Assessment Condition Summary:
Internal Audit determined that the IT department does not follow a set of information technology standards. Standards provide a framework organizations can use to design effective controls to ensure a secure information system infrastructure.

Criteria:
UTA Department of Information Technology No. 9.1.1 IT Application and Systems Devops Policy states:
I. Purpose.

> *A goal of the IT Department is to provide quality systems for users that initially meets the users requirements and is without issues. Secondary to this goal, it is also a goal to develop systems that are easily supportable and understandable by IT staff assigned to support systems. To this end, this Policy establishes the minimum requirements, responsibilities used to successfully develop and deploy applications and systems, and to establish best practices and procedures for ongoing Application services and Database support. Detailed procedures may exist in supportive Application Support and Development Division Standard Operating Procedures (SOPs).*

Utah Code Part 7 Cybersecurity Affirmative Defense Act states:
78B-4-703 Components of a cybersecurity program eligible for an affirmative defense

> *(1) Subject to Subsection (3), a person's written cybersecurity program reasonably conforms to a recognized cybersecurity framework if the written cybersecurity program:*
>
> *(a) is designed to protect the type of personal information obtained in the breach of system security; and*
>
> *(b)*
>
> *(i) is a reasonable security program described in Subsection (2);*
>
> *(ii) reasonably conforms to the current version of any of the following frameworks or publications, or any combination of the following frameworks or publications:*
>
> *(A) NIST special publication 800-171;*
>
> *(B) NIST special publications 800-53 and 800-53a;*
>
> *(C) the Federal Risk and Authorization Management Program Security Assessment Framework;*
>
> *(D) the Center for Internet Security Critical Security Controls for Effective Cyber Defense; or*
>
> *(E) the International Organization for Standardization/International Electrotechnical Commission 27000 Family - Information security management systems;*
>
> *(iii) for personal information obtained in the breach of the system security that is regulated by the federal government or state government, reasonably complies with the requirements of the regulation, including:*
>
> *(A) the security requirements of the Health Insurance Portability and Accountability Act of 1996, as described in 45 C.F.R. Part 164, Subpart C;*
>
> *(B) Title V of the Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, as amended;*

(C) the Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283;
(D) the Health Information Technology for Economic and Clinical Health Act, as provided in 45 C.F.R. Part 164;
(E)Title 13, Chapter 44, Protection of Personal Information Act; or
(F) any other applicable federal or state regulation; or

(iv) for personal information obtained in the breach of system security that is the type of information intended to be protected by the PCI data security standard, reasonably complies with the current version of the PCI data security standard.

(2) A written cybersecurity program is a reasonable security program under Subsection (1)(b)(i) if:

(a) the person coordinates, or designates an employee of the person to coordinate, a program that provides the administrative, technical, and physical safeguards described in Subsections 78B-4-702(4)(a) and (c);

(b) the program under Subsection (2)(a) has practices and procedures to detect, prevent, and respond to a breach of system security;

(c) the person, or an employee of the person, trains, and manages employees in the practices and procedures under Subsection (2)(b);

(d) the person, or an employee of the person, conducts risk assessments to test and monitor the practice and procedures under Subsection (2)(b), including risk assessments on:

(i) the network and software design for the person;
(ii) information processing, transmission, and storage of personal information; and
(iii) the storage and disposal of personal information; and

(e) the person adjusts the practices and procedures under Subsection (2)(b) in light of changes or new circumstances needed to protect the security, confidentiality, and integrity of personal information.

(3)

(a) If a recognized cybersecurity framework described in Subsection (1)(b)(ii) or (iv) is revised, a person with a written cybersecurity program that relies upon that recognized cybersecurity framework shall reasonably conform to the revised version of the framework no later than one year after the day in which the revised version of the framework is published.

(b) If a recognized cybersecurity framework described in Subsection (1)(b)(iii) is amended, a person with a written cybersecurity program that relies upon that recognized cybersecurity framework shall reasonably conform to the amended regulation of the framework in a reasonable amount of time, taking into consideration the urgency of the amendment in terms of:

(i) risks to the security of personal information;
(ii) the cost and effort of complying with the amended regulation; and
(iii) any other relevant factor.

Inherent Risk:
Absent the guidance of a reputable framework, internal controls over key information systems may not be designed adequately to protect private information from intrusion and exploitation, or to ensure the stability and fidelity of the system.

Cause:
The previous Director of IT had stated on several occasions,

"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."

Recommendations:
IA recommends UTA implement a set of standards or framework to provide assurance that:

- The IT department is governed and managed holistically
- Gaps in controls are identified and addressed
- UTA has guidance in areas of regulatory compliance, risk management and aligning IT Strategy with organizational goals.

Management Response and Action Plan:
Management will develop a process to better align I.T. with a reputable Framework. As the process is developed and gaps identified, management will determine what additional Risk Management Activities need to be implemented. I.T. Management will identify areas that would benefit from aligning I.T. Strategy with Organizational Goals.

Target Completion Date:
March 31, 2023

Current Status – Audit Phase:
Partially implemented.

Management has procured a new software that will aid in monitoring against NIST standards. This a strong first step toward standards compliance.

Current Status – Follow-up Phase:
Completed.

IT management adopted the NIST Cybersecurity Framework. Management hired a third-party, Optiv, to perform an assessment and analysis of conformance with the Standards, with a report issued November 27, 2024. Management addressed the issue, and IA closed it as completed.

Management Response – Follow-up Phase
Management did not provide a response.